**FACULDADE DE TECNOLOGIA**
**DE SÃO JOSÉ DO RIO PRETO**

# ENGENHARIA SOCIAL: MÉTODOS DE PREVENÇÃO, MITIGAÇÃO E EXECUÇÃO ÉTICA

**MARIANA MELLO DE SOUZA**

**Orientador**
**Prof. Carlos Magnus Carlson Filho**

**Coorientador**
**Prof. Juliano Farias de Nóbrega**

**São José do Rio Preto**
**2024**

# FACULDADE DE TECNOLOGIA
# DE SÃO JOSÉ DO RIO PRETO


# ENGENHARIA SOCIAL: MÉTODOS DE PREVENÇÃO, MITIGAÇÃO E EXECUÇÃO ÉTICA


**Mariana Mello de Souza**


**Trabalho de Graduação apresentado à Faculdade de Tecnologia de São José do Rio Preto como requisito parcial para obtenção do grau de Tecnólogo em Informática para Negócios, sob a orientação do Prof. Carlos Magnus Carlson Filho e coorientação do Prof. Juliano Farias de Nóbrega.**


**São José do Rio Preto**
**2024**

# FACULDADE DE TECNOLOGIA
# DE SÃO JOSÉ DO RIO PRETO

## Banca Examinadora

Menção: _____ em _____/_____/_____

Nome:_____ Assinatura:_____

Nome:_____ Assinatura:_____

Nome:_____ Assinatura: _____

**São José do Rio Preto**
**2024**

# DEDICATÓRIA

Dedico este trabalho a todos que me incentivaram na vida e quem me incentivou em cibersegurança, em especial aos meus pais – Alaide e Hugo - e aos meus professores da FATEC – todos, mas em especial aos professores Carlos, Juliano e Paulo, do qual esse último, mesmo lecionando Redes, indiretamente me fez me descobrir qual rumo iria seguir dentro da Tecnologia, além do João e Ademar, um dos que me animaram para que eu chegasse até o final do curso. Graças a vocês que confiaram em mim, dedico o resultado do esforço realizado ao longo deste percurso. Me sinto agraciada por estar formando minha vida acadêmica no ombro de gigantes.

# RESUMO

Esse trabalho de Conclusão de Curso aborda o tema da Engenharia Social, um tipo de invasão que não envolve erros computacionais ou falhas, mas sim explora vulnerabilidades e instintos humanos para coletar dados sigilosos e confidenciais. É um dos métodos mais antigos de ataque cibernético, e que até hoje ainda se mostra eficaz. O artigo inicia com o conceito de Engenharia Social, traçando sua história ao longo do tempo, e sua importância na cibersegurança, e como foi desenvolvido as variantes de engenharia social de ordem cronológica. O trabalho abordará as metodologias de prevenção e mitigação que pode ser usado numa empresa, baseado nas normas ISO 27000, trazendo à tona métodos como treinamento, a criação de políticas de segurança numa empresa e a importância de uma cultura voltada na proteção de dados e a segurança. Por último, faremos um estudo detalhado, onde uma simulação de ataque de engenharia social é feita em um ambiente controlado, e os resultados são usados para sugerir melhorias. Sempre temos que se atentar aos principais métodos de engenharia social, incluindo o *phishing*, *quid pro quo*, *pretexting*, *baiting* e *tailgating*, e estratégias de prevenção, baseado nas normas *ISO* mais atuais e na família *ISO 27000*, e mitigação dos problemas, usando métodos práticos de como impedir esses ataques.

**Palavras-Chave:** Engenharia Social, phishing, pretexting, baiting, tailgating, prevenção, ISO 27000, mitigação, Segurança da Informação, Execução, Ética.

# ABSTRACT

*The main purpose was a discussion and investigating social engineering, a type of invasion that does not involve computer errors or flaws but rather exploits vulnerabilities and human instincts to collect sensitive and confidential data. It is one of the oldest methods of cyber-attack, and it remains effective today. The article begins with the notion of Social Engineering, tracing its development over time, its significance in cybersecurity, and the sequential development of its variants. Finally, we will carry out a detailed study, where a simulation of a social engineering attack is carried out in a controlled environment, and the results are used to suggest improvements. We always must be aware of the main methods of social engineering, including phishing, quid pro quo, pretexting, baiting and tailgating, and prevention strategies, based on the most current ISO standards and the ISO 27000 family, and mitigation of problems, using practical methods of how to prevent these attacks. Based on the above-mentioned findings, it can be said that prevention and mitigation methodologies, based on the ISO 27000 standards, can be effectively implemented in a company. These include training, the creation of security policies, and fostering a culture that prioritizes data protection and security.*

**Keywords:** *Social Engineering, phishing, pretexting, baiting, tailgating, prevention, ISO 27000, mitigation, Information Security, Execution, Ethics.*

# SUMÁRIO

## LISTA DE ABREVIATURAS

ISO: Organização Internacional para Padronização (*International Organization for Standardization*).

IEC: Comissão Eletrotécnica Internacional (*International Electrotechnical Commission*).

NIST: Instituto Nacional de Padrões e Tecnologia (*National Institute of Standards and Technology*).

STIG: Guias de Implementação Técnica de Segurança (*Security Technical Implementation Guide).*

TI – Tecnologia da Informação.

LGPD - Lei Geral de Proteção de Dados.

EGD - Estratégia de Governança Digital.

E-Ciber: Estratégia Nacional de Segurança Cibernética.

OMB: Gabinete de Gestão e Orçamento (*Office of Management and Budget*).

OSINT: Inteligência de Fontes Abertas (*Open Source Intelligence*).

DSIC: Departamento de Segurança da Informação e Cibernética.

GSIPR: Gabinete de Segurança Institucional da Presidência da República.

DISA: Agência de Sistemas de Informação de Defesa (*Defense Information Systems Agency*).

MFA: Autenticação Multifator.

CISA: Agência de Segurança de Ciberinfraestrutura (*Cybersecurity and Infrastructure Security Agency*).

PII: Informações Pessoais Identificáveis (*Personally Identifiable Information*).

CSIRT: Equipe de Resposta a Incidentes de Segurança em Computadores (*Computer Security Incident Response Team).*

IDS: Sistema de Detecção de Invasão (*Intrusion Detection System*).

IPS: Sistema de Prevenção de Invasão (*Intrusion Prevention System*).

HTML: Linguagem de Marcação de HiperTexto (HyperText Markup Language).

SMTP: Protocolo de Transferência de Correio Simples (*Simple Mail Transfer Protocol*).

URL: Localizador Uniforme de Recursos (Uniform Resource Locator).

IP: Protocolo de Rede (Internet Protocol).

# LISTA DE FIGURAS

# INTRODUÇÃO

Nas últimas décadas, a tecnologia se tornou cada vez mais democratizada, acessível, usada e aprimorada, renovando a maneira como indivíduos e empresas otimizam seus processos. Todavia, à medida que a tecnologia avança, os ataques cibernéticos também se aprimoram e encontram novas brechas de ataque. Um dos métodos mais perigosos e, coincidentemente, utiliza-se menos de falhas tecnológicas e mais de vulnerabilidade e ingenuidade humana, é a engenharia social, baseado, além de técnica de ciberataque, como uma forma de manipulação psicológica para vazar dados sensíveis. Resumidamente, de acordo com Mitnick e Simon (2002), a engenharia social é "a arte de enganar as pessoas para que revelem informações confidenciais".

Diferentemente de ciberataques que usam técnicas de *hacking* ou malwares complexos, aqui, a engenharia social tem uma estrutura relativamente simples, se alimentando de manipulação psicológica para que as vítimas forneçam, sem perceber, dados de login, cartão de crédito, cartão de débito, *PIX*, *IPs*, dinheiro, dados bancários, dados confidenciais de empresas etc. E isso pode ser explorado por diversas técnicas de engenharia social, como *phishing*, quid pro quo, *pretexting*, *baiting* e *tailgating*. Em uma empresa, a situação pode se tornar avassaladora, com custos com violações de dados, perder reputação e ter que investir em medidas de recuperação (HERLEY, 2021).

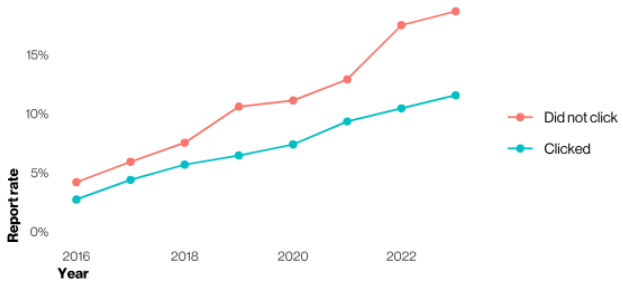



Figura 1. Taxa geral de relatório de Phishing por e-mail ao longo dos anos.

Essa técnica só é bem-sucedida e até hoje muita gente cai nela, além de ter repercussão nas mídias, pois os seres humanos são e continuam sendo o elo mais fraco na cadeia de proteção (HADNAGY, 2011). Segundo *Verizon Data Breach Investigations Report* (2023), 68% das violações de segurança envolvem algum tipo de erro humano, e é continuamente associado a engenharia social. Além disso, apoia-se numa estratégia velha e conhecida de manipulação humana, a manipulação emocional, por vários meios: *Cialdini* (2001) identifica

seis princípios psicológicos frequentemente usados em técnicas de persuasão: reciprocidade, compromisso, coerência, validação social, afeição, autoridade e escassez. Na prática, é refletida na engenharia social com os seguintes métodos: da impressão de autoridade para não parecer farsante, pegando confiança da vítima até ela cair na armadilha, o senso de urgência, o medo e coerção, a curiosidade do usuário, pegando uma causa nobre para explorar a empatia da vítima, a ganância em descontos enormes ou promessas de ganhos rápidos de dinheiro, fazendo reciprocidade com a vítima, isolando a vítima para que a transação entre eles fiquem em sigilo, fingindo ser alguém da família ou trabalho, entre outros.

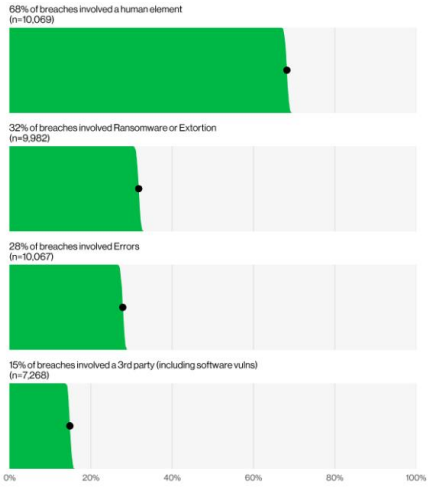



Figura 2. 68% dos ataques cibernéticos tem algum erro e fator humano envolvido.

Um exemplo a se lembrar foi o que ocorreu em 2020, no Twitter, onde várias contas, incluindo perfis de figuras públicas, como Barack Obama, Jeff Bezos, Kanye West, Floyd Mayweather e Elon Musk, e empresas como *Apple* e *Uber* foram afetadas por meio de um ataque de *spear phishing*, que ocorreram com os funcionários internos da empresa, que foram enganados, expondo dados de 350 milhões de contas e os hackers ganharam cerca de US$ 110 mil durante o golpe. Alexander (2020) específica que o *spear phishing*, como no caso do ocorrido no *Twitter*, o fator que se caracteriza como diferenciação em relação ao *phishing*, é que o ataque ocorre com indivíduos ou organizações específicas, com mensagem personalizada para aumentar a credibilidade.

Outro exemplo a se citar é a *Uber*, hackeado em 2022, a empresa tirou do ar temporariamente seus sistemas internos de comunicação e engenharia, entre eles o sistema *Slack*, e no momento do ataque, os funcionários foram instruídos a não usar os sistemas

internos de comunicação. Uma conta *Slack* de um colaborador foi comprometida e enviou mensagens para a equipe interna de que a *Uber* foi invadida e expôs vários bancos de dados internos.

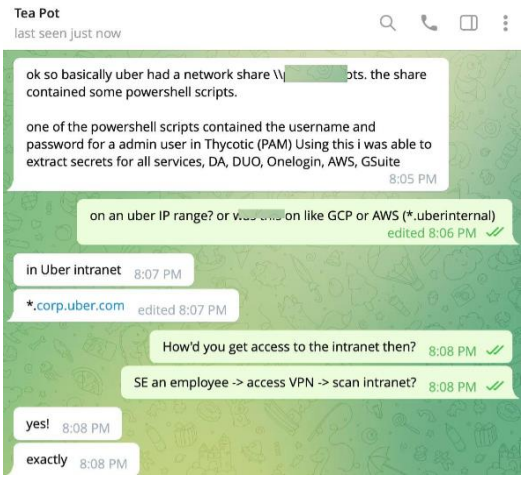



Figura 3. *Printscreen* de uma conversa privada com o *hacker* no *Telegram*

A prevenção contra engenharia social necessita de mais do que apenas sistemas de segurança. Treinamento dos funcionários, uma política de segurança mais robusta, adoção de autenticação em dois fatores, monitorar ameaças, verificação e autenticação de solicitações, simulações de ataques de engenharia social feita por um *pentester*, gerenciador de senhas e respostas rápidas a incidentes também é crucial para a prevenção. De acordo com um estudo da IBM (2023), o custo médio de uma violação de dados por engenharia social é, aproximadamente, 4,45 milhões de dólares, o que se faz necessário sua prevenção.

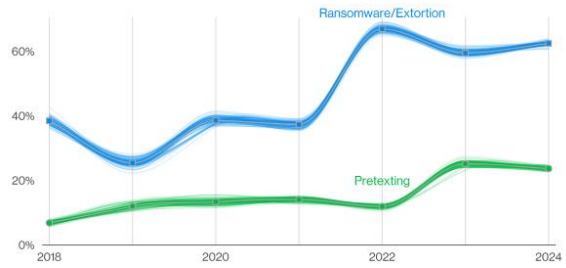



Figura 4. Variedades de ação em motivação financeira ao longo do tempo. Dá para se notar que *Pretexting*, embora seja menor que *Ransomware*, também teve um aumento entre 2018 até 2024.

A ética e legalidade da engenharia social também é um ponto a se pôr na discussão, pode ser usado tanto de forma negativa, para expor dados ilegalmente de uma empresa, quanto também de forma legítima, especialmente em equipes *red team*, para testar suas defesas em empresas. Ainda assim, nem sempre os ataques ilegais de engenharia social se resumem apenas a fraqueza humana, muitas vezes, envolvem planejamento calculado pré-ataque, algumas informações antecipadas sobre a vítima e a criação de cenários convincentes.

Esse presente artigo irá abordar três pontos: Prevenção, Mitigação e Execução. Na primeira etapa, será citado as formas mais comuns de ciberataques de engenharia social, bem como maneiras de se prevenir desses ataques, e conhecimento sobre a norma ISO 27000 para entender como agir nesses casos.

A segunda etapa é a mitigação, será destrinchado as ações que podem ser tomadas em um ciberataque em tempo real, e quais políticas implantar para diminuir os impactos. Será pego também casos reais de empresas que sofreram ataques de engenharia social e o que foi feito para resolver o problema, ao ponto de não comprometer, ou comprometer o mínimo possível, dos dados existentes durante a invasão.

Por último, será tratado sobre a execução, como são feitos esses ataques, como se utiliza o Social Engineering Toolkit (SE Toolkit ou SET), theHarvester, GoPhish, BeEF e ReconNg, e como é elaborado um ambiente de simulação de ataque de engenharia social em uma empresa, num ambiente controlado.

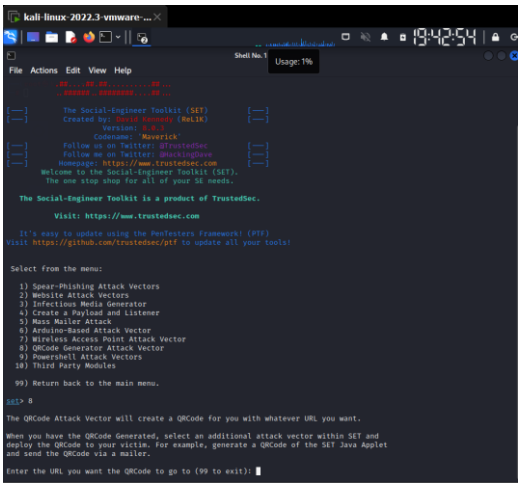



Figura 5. Tela do SET (Social Engineering Toolkit)

# CAPÍTULO 1. FUNDAMENTAÇÃO TEÓRICA

Esse artigo tem como fundamentação teórica todo o conceito de Engenharia Social. A pesquisa será baseada nas pesquisas, artigos e livros clássicos e atuais, em obras teóricas e práticas com autores renomados, como Kevin Mitnick, Christopher Hadnagy, Peter Yawoski, entre outros.

A engenharia social é um conjunto de técnicas de manipulação psicológica que usam fraquezas emocionais, comportamentais e cognitivas, e baseadas principalmente nos princípios citados por Cialdini (2006), reciprocidade, comprometimento, validação social, autoridade, escassez e simpatia, bastante presente nesses ciberataques, para manipular suas vítimas e, consequentemente, obter dados sigilosos. Segundo Mitnick e Simon (2002), o sucesso desse tipo de ataque reside no fato de que o elo mais fraco na segurança de qualquer sistema é o ser humano. Uma violação desse porte numa empresa, não apenas se torna corrosivo, como também pode fazer a empresa ter problemas com as regulamentações, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, o Regulamento Geral de Proteção de Dados (GDPR) na Europa, e A Lei de Proteção e Privacidade de Dados dos EUA (ADPPA).

Na história, a engenharia social tem origem em golpes que sempre foram comuns na sociedade, mas que, posteriormente, se compactuou na internet. Sua evolução é diretamente proporcional ao avanço da tecnologia, e com o advento das redes sociais, se tornou mais usada, já que as pessoas se tornaram mais expostas a manipulação na web de forma geral. Agora, com o advento da IA e dos DeepFakes, há um potencial futuro e evolutivo da engenharia social nesse meio, o que torna a situação preocupante, abusando ainda mais do fator manipulativo e das tecnologias mais atuais. Essa preocupação inclusive, é compartilhada por Hadnagy (2011), que destaca a crescente sofisticação dos métodos de engenharia social.

- **Normas ISO Utilizadas**

Como citado anteriormente, a ISO ideal e que tange a organização das empresas em relação a Segurança da Informação é a família 27000, especialmente a 27001 e 27002. Na etapa da prevenção, é a adequada para esse caso. A ISO/IEC 27001 estabelece requisitos para implementar, manter e melhorar o sistema de SGSI. Também estabelece definições para como proceder em ação corretiva, ameaças, e incidentes de segurança da informação, além de

minimizar vulnerabilidades humanas que podem causar engenharia social. Conjunto a essa norma, está a 27002, oferecendo para a 27001 um conjunto de práticas para controle desses incidentes, para garantir a confidencialidade, integridade e disponibilidade dos dados.

Outras normas que também fornecem suporte é a 27005:2018, 27017:2015 e 27018:2019. A 27005 é uma complementação da 27002, focando no gerenciamento generalizado de riscos de segurança da informação, avaliação, tratamento, aceitação e segurança deles. A 27017 fornece diretrizes de controle de segurança para acessos em nuvem, orientando a implementação adicional de 37 controles especificados e 7 relacionados ao serviço em nuvem, verificando quem é o responsável pelo que vai entre o provedor de serviços e o cliente na nuvem, a remoção ou devolução de ativos, configuração de máquinas virtuais, proteção do ambiente virtual do cliente, procedimentos administrativos sobre a nuvem, monitorar atividade do cliente em nuvem, e sobre alinhar ambiente virtual de rede e de nuvem. Paralelo a isso, tem a 27018, que trata sobre um conjunto comum de categorias e controles que pode ser implementado por um provedor de serviços em nuvem, como um processador de PII, auxiliando o provedor, verificando se suas obrigações são diretas ou por contrato, auxilia o cliente e o processador de PII ao fazer um acordo contratual, prover ao cliente um mecanismo para exercer direitos e responsabilidades de auditoria, e a transparência em assuntos relevantes dentro da nuvem.

- **Ferramentas e Softwares Utilizados**

Na etapa de prevenção, será focado em alguns programas que podem ser usados facilmente por qualquer pessoa em qualquer grau de conhecimento, como plataformas de e-learning, como KnowBe4 e SANS Security Awareness, aplicativos de autenticação multifator, como Microsoft Authenticator, criptografia de dados com BitLocker, ferramentas de DLP (Data Loss Prevention), como Symantec DLP, e gerenciamento de direitos digitais (DRM).

Na etapa da Execução, seria usado ferramentas predominantemente em sistema Linux, como Ubuntu, Kali Linux e Arch Linux, e será o Social Engineering Toolkit (SE Toolkit ou SET), o GoPhish, BeEF e ReconNg, MalteGo e o PhishMe para avaliar as respostas dos funcionários mediante a uma simulação de ataque. Serão tanto ferramentas de engenharia social, como também coleta de dados.

- **Princípios de Controle de Acesso**

Há bastante métodos para a prevenção contra uma engenharia social, e uma delas é o Princípio do Menor Privilégio (Principle of Least Privilege). Segundo Brown (2013), esse princípio é, nada mais e nada menos, que o controle de acesso precisa ser adicionado de forma que cada cargo dentro do sistema, em uma corporação, receba a quantidade mínima de recursos de sistema para trabalhar, apenas incluindo o necessário. Portanto, fazer isso evita erros, acidentes ou ato não autorizado. Brown (2013) também acentua a autenticação para se acessar ao sistema, para provar que o usuário é autêntico, o uso de políticas fechadas, isto é, somente acessos autorizados a determinados itens secretos são permitidos, separar deveres de sistema na empresa, para que o gerenciamento do sistema não fique concentrado na mão de apenas uma pessoa, adicionar políticas de segurança na empresa, e políticas administrativas, além de citar 3 tipos de políticas possíveis em controle de acesso, Controle de acesso discricionário (Discretionary Access Control — DAC), Controle de acesso mandatório (Mandatory Access Control — MAC) e Controle de acesso baseado em papéis (RBAC).


Figura 6. Essas políticas não são exclusivas e podem ser utilizadas mais de uma política em um sistema, para alguns ou todos os acessos da empresa.

O controle de acesso direcionado funciona da seguinte maneira: uma pessoa pode receber direitos de acesso que possibilita com que ela, por sua vontade, possa habilitar outro colaborador a acessar algum recurso. O sistema mais comum para esse tipo de abordagem para se usar no banco de dados é a matriz de acesso. A matriz de acesso foi arquitetada por

Lampson (1969 e 1974) e aprimorado por Graham e Denning (1972) e Harrison et al. (1976) e é decomposto em um de dois módulos, por colunas, formando lista de controle de acessos.

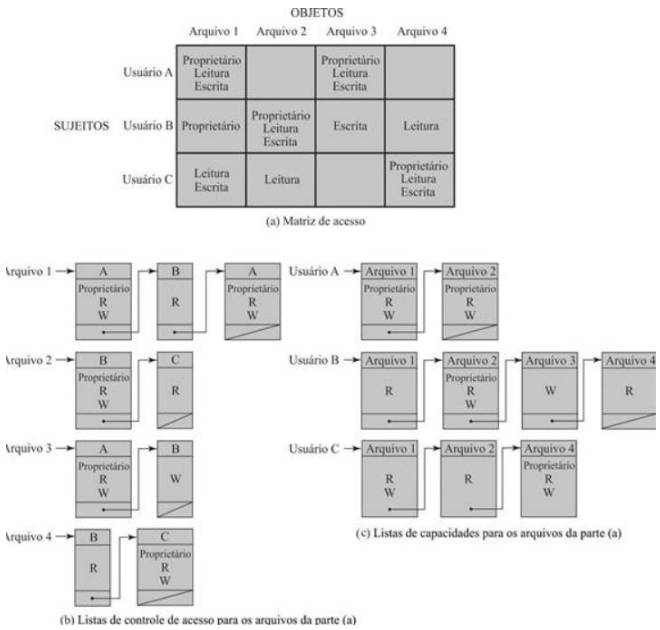



Figura 7. Exemplo de controle de acesso simples.

Política de Expiração de Sessão: é uma medida de segurança que limita o tempo que um usuário pode se autenticar durante períodos de inatividade e deve se autenticar novamente, evitando ataques em sessões não monitoradas. De acordo com a ISO/IEC 27001:2013, as empresas precisam implementar controles para minimizar o uso prolongado de sessões, especialmente sessões inativas. O NIST (*National Institute of Standards and Technology*) também recomenda essas práticas de timeout automático para reduzir ataques de pessoas de fora da empresa (GRASSI, Paul A. et al., 2017).

Autenticação multifator: Ele adiciona camadas extras de segurança ao exigir vários métodos de verificação antes de autenticar no sistema da empresa. Pode ser uma mistura de senha, token, pin, biometria etc. Segundo NIST (2020), ela é considerada uma das práticas mais eficazes para verificação, e reduz o acesso não autorizado mediante credenciais roubadas de algum funcionário da empresa. Esse assunto também é abordado na ISO/IEC 27001:2013.

- **Tipos de Engenharia Social**

Há vários métodos do quais podem ser usados para executar uma engenharia social. Algumas das técnicas incluem:

*Phishing*: Seu nome deriva-se da palavra "*fishing*" (pescar), no inglês, já que o ataque é semelhante ao ato de pescar, nesse caso, "pescar" (enganar) vítimas. Um dos métodos mais comuns, pode ser realizado por meio de e-mail ou mensagens, para que as vítimas, sem querer e ingenuamente forneçam senhas ou dados financeiros (JAKOBSSON; MYERS, 2006). Tem algumas variantes, como o *Phishing* por e-mail, *smishing*, *pharming*, *vishing*, *spear phishing*, *whaling*, *phishing* com inteligência artificial.

*Phishing* por e-mail: Uma forma clássica e antiga de *phishing*, o criminoso envia e-mails que parecem de fontes confiáveis, como empresas conhecidas e renomadas, mas na verdade é um golpe de *Phishing*. Na maioria dos casos, contém um link que pedem informações confidenciais quando abertos, ou arquivos que instalam *malware*.

*Smishing*: Um tipo de *phishing* que utiliza *SMS*. O cibercriminoso envia uma mensagem se passando por uma empresa renomada, instituição financeira, e colocando um link, para que a pessoa acesse, mande os dados bancários e confidenciais, ou receba um *malware* no seu dispositivo.

*Pharming*: O atacante envia a vítima de uma página verdadeira para outra falsa, ou por meio de malware que altera o arquivo de hosts do computador, ou envenenamento de DNS, conseguindo modificar a tabela *DNS* de um servidor. É uma forma mais sutil de *phishing* pois não existe um convite para um site.

*Vishing*: Também conhecido como *Voice Phishing*, é feito por meio de ligação, onde o criminoso incorpora uma suposta empresa renomada, induzindo a pessoa a passar senhas, número de cartão de crédito e dados sensíveis.

*Spear Phishing*: Normalmente acontece esse ataque com grandes corporações ou pessoas executivas, de renome ou status social. Há um uso detalhado dos dados sobre o alvo para que a mensagem seja o mais convincente possível, normalmente retirados de redes sociais, sites da empresa etc. É bastante executado já que as informações obtidas podem manchar e causar prejuízos a empresa vítima.

*Phishing* com Inteligência artificial: É usado ferramentas como *Play.ht, Murf.AI, Speechify, Listnr, LOVO (Genny)*, *Synthesys*, dentre outros, para ficar ainda mais fidedigno os ataques de *phishing* e ser mais fácil de enganar.

*Pretexting*: A criação de uma situação fictícia para enganar a vítima, para que ela acredite que está conversando com uma autoridade legítima (HADNAGY, 2011).

*Baiting*: Um método de isca, onde a vítima é atraída por ofertas ou recompensas atraentes, fazendo assim, com que a vítima, sem perceber, baixe *malware* no seu computador, ou forneça dados sensíveis, ou então, *pendrives* infectados (SYMANTEC, 2021).

*Tailgating*: Mais utilizadas em ataques físicos, em que a pessoa mal-intencionada acaba tendo acesso a áreas restritas, ao seguir uma pessoa autorizada, em uma empresa com falta de segurança e validação de credenciais e documentos (HADNAGY, 2018).

*Quid pro Quo*: Baseado na frase latina "algo para algo", é similar aos métodos *phishing* e *baiting*, porém, sua diferença está no fato de que o golpista tenta convencer a vítima que ele está fazendo um favor a ela, logo, a vítima "deveria se sentir grata" em contribuir com ele. (HADNAGY, 2018).

*Scareware*: induz a vítima pelo medo, para que ela realize uma ação. Um exemplo prático que existe são os sites que exibem tela de "Encontrado 8 vírus no seu computador, seu computador está em risco" ao abrir um link pirata de *apk* grátis no Youtube. A vítima, por medo, clica, instala para tentar remover o suposto "vírus", que não existe, pois é um alerta falso. (SYMANTEC, 2021).

*Watering Hole*: Nesse caso, há a invasão de um site verdadeiro, acessado por um público específico, infectando o site com *malware* e para que os usuários coloquem sem perceber nos seus dispositivos, para que o público acesse e nem saiba que o site foi atacado. (SYMANTEC, 2021).

- **Métodos de coletar informação**

Open Source Intelligence (OSINT): Coleta de informações por fontes públicas e disponíveis na internet, como sites governamentais, redes sociais, entre outros, reunindo informações sobre usuários ou empresas que podem ser usados para realizar ataques de engenharia social.

Dumpster Diving: Vasculhar o lixo de uma empresa para coletar informações, como documentos, notas etc. Ele é um método antigo, simples, mas pode ser eficaz em empresas que não seguem e/ou desconhecem boas práticas de cibersegurança.

# CAPÍTULO 2. DESENVOLVIMENTO

- **Metodologia**

### 2.1.1 Tipo do trabalho

Esse presente artigo usa uma abordagem quantitativa, explicativa e aplicada, aprofundando sobre as várias variantes de engenharia social, seus métodos, seus impactos na sociedade e como prevenir contra isso, além de como usar a engenharia social de forma ética, para aumentar a segurança nas empresas. Como o tema ainda está em fase de aprofundamento e visando que é um tema que evolui de acordo com a tecnologia, ou seja, muda rapidamente, o objetivo do artigo é trazer soluções práticas e abrangentes.

### 2.1.2 Coleta de dados

Pesquisa Bibliográfica: Será coletado fontes de livros de segurança da informação, artigos científicos, sites acadêmicos e jornais acadêmicos. Terá uma revisão teórica sobre o que é e como funciona a engenharia social, para aprofundar o conhecimento na área e para alcançar um determinado público que está nos meios acadêmicos ou pensa em se aperfeiçoar em cibersegurança. Iremos identificar técnicas relacionadas e conceitos sobre o tema. As fontes serão pegas pelo Google Scholar, IEEE, CAPES, Ric CPS, site da UnB, entre outros.

### 2.1.3 Desenvolvimento

Os softwares que serão utilizados no exemplo prático serão predominantemente no sistema Linux, em especial sistemas operacionais como Ubuntu, Kali Linux, e ferramentas como Social Engineering Toolkit, GoPhish, BeEF, ReconNg e MalteGo

Todo o material utilizado na pesquisa, será referenciado conforme as normas do ABNT, com seus respectivos links de acesso.

### 2.1.4 Recursos

Computadores próprios, periféricos próprios, internet doméstica, livros digitais e físicos próprios.

### 2.1.5 Artigos Similares

O campo de estudo sobre a engenharia social já é ativo e está presente em uma parte considerável do setor acadêmico. Portanto, há alguns artigos similares que já abordam esse problema, assim como esse presente artigo. Aqui, irei referenciá-los, e mostrar quais são os pontos convergentes e divergentes de cada um, assim como alguns tópicos não abordados.

**Explorando a Engenharia Social com Social Engineering Toolkit - Faculdade de Tecnologia de Americana, Tecnologia em Segurança da Informação (SALES et al, 2023)**

Esse artigo apresenta alguns pontos em comum que seria interessante destacar, como similaridade: O uso do Social Engineering Toolkit, algumas fontes similares como Hadnagy, Kapersky, uso de Kali Linux e leis Brasileiras.

As diferenças são: O trabalho de Sales (2023) é mais nichado, enquanto nesse em questão foi mais abrangente. O uso de simulação de Phishing com e-mail foi feito, mas no caso, Sales (2023) usa o próprio SET, enquanto nesse trabalho em questão, usamos GoPhish, usando o SET para outra finalidade. Houve mais aprofundamento na ISO/IEC e STIGs nesse nosso trabalho em questão, assim como houver a abordagem das normas NIST e sobre as técnicas OSINT. Não houve quaisquer enfoques em prevenção e mitigação relacionado a empresas, indicando que o trabalho de Sales (2023) é mais voltado para estudantes de cibersegurança, enquanto nosso público-alvo são estudantes e entusiastas de cibersegurança e quem pensa em montar empresas.

**A Brecha humana da Segurança da Informação: Engenharia Social e Políticas de Segurança. Faculdade de Tecnologia de Americana, Tecnologia em Segurança da Informação (RODRIGUES, 2018).**

Dos trabalhos de Graduação das FATECs, esse foi o mais completo encontrado, um trabalho monográfico envolvendo um estudo de caso, e o único trabalho que eu vi citar NIST e SANS Institute, felizmente o trabalho não foi apenas com livros brasileiros. Suas semelhanças são: Citações de Leis Brasileiras, de Kevin Mitnick e Simon (2003), além dos já citados anteriormente.

Diferenças: Seu trabalho foi mais exploratório do que informativo, baseando em pesquisa de campo de autoria deles, de alguns empresários. Houve menos aprofundamento em prevenção e mitigação, não houve a parte de execução, sendo seu trabalho uma amostragem da realidade atual, sobre se os empresários coletados na pesquisa sabiam de alguma forma sobre como implantar medidas preventivas na sua própria empresa. O nosso trabalho foi mais nichado, mais informativo, mais preventivo e com público-alvo mais segmentado (estudantes e entusiastas de cibersegurança e quem pensa em montar ou tem empresas), enquanto seu público-alvo seria empresários e montar uma amostra da realidade de forma estatística para acadêmicos. O trabalho de Rodrigues (2018) teve menção de ITSEC, COBIT, OCDE e ITIL, enquanto o nosso teve menção de STIGs.

**Fatores humanos em cibersegurança: uma revisão sistemática da literatura – Universidade Federal de Uberlândia, Bacharel em Sistemas de Informação (TAKEUCHI, 2023)**

Artigo mais voltado para o meio acadêmico e mais aprofundado em psicologia, também é mais exploratório. Aqui, ele revisa artigos acadêmicos sobre esse tema baseado em 3 perguntas: associação ao tema proposto, quais os fatores humanos apontados e como se relacionam, e se tem conjuntos consolidados de boas práticas. As semelhanças são: enfoque em prevenção.

As diferenças são: Nosso artigo teve a citação de NIST, STIGs, ISO/IEC, Leis Brasileiras e Americanas, bem como a etapa de execução e sugestões de aplicativos tanto para mitigação quanto para a execução, de vários níveis de conhecimento, um treinamento inteiro montado detalhadamente com a ajuda das normas NIST, assim como a citação de Cialdini (2006) sobre princípios psicológicos utilizados que ajudam em uma tentativa de persuasão, usado em engenharias sociais. O artigo de Takeuchi (2023) teve a citação de Big Five, é mais exploratório, mais voltada a área acadêmica, público mais nichado, voltado a acadêmicos e entusiastas de cibersegurança, não houve etapa de execução.

## 2.2 Prevenção e Mitigação

Na parte da prevenção e Mitigação, separamos o desenvolvimento em algumas etapas, para ser mais compreensível e estruturado diante do processo de construção da nossa pesquisa. Esses são os tópicos:

- Conscientização dos usuários baseado na Norma NIST;

- Política de Privacidade, Controle de Acesso e *STIGs*;

- Autenticação Multifator;

- Boas práticas de descarte de informações;

- Resposta a Incidentes, Recuperação e Análise pós-incidente;

- Uso de Tecnologia e Ferramentas de Segurança;

### 2.2.1 Conscientização dos Usuários baseado na norma NIST

Tudo começa com a conscientização, especialmente quando se trata de um ataque de cibersegurança que usa como fraqueza o fator humano. Para se prevenir, a empresa deve investir em treinamentos, especialmente aquelas baseadas em NIST 800-50 e NIST 800-16. Segundo a norma NIST, há 3 etapas do treinamento de segurança de tecnologia da informação: montar o plano de treinamento (incluindo o desenvolvimento do ensino de segurança da informação), desenvolver o conhecimento e o material de treino, e implementar o programa.

Um desenvolvimento de um programa de treinamento e conhecimento numa empresa precisa ser arquitetado, desenvolvido, e implantado de várias formas diferentes. Segundo a NIST (2003), há 3 modelos possíveis, o Modelo de Gestão de Programas Centralizado, onde a organização do treinamento de segurança da informação é responsabilizada por uma autoridade central; o Modelo de Gestão de Programas Parcialmente Descentralizado, onde é designado por autoridades responsáveis para criar o treinamento, mas são mais de um responsável; e o Modelo de Gestão de Programas Totalmente Descentralizado, onde a autoridade do projeto (normalmente o CIO ou o administrador do programa de segurança da informação), distribui a responsabilidade para várias diretorias de autoridade, que por sua vez, são submissas a autoridade central.

É preciso criar uma equipe de avaliação de necessidades, onde participa o Gestor Executivo (gerenciador do projeto), a equipe de segurança (uma equipe treinada em segurança da informação), Gerenciadores do Sistema (que provavelmente tem uma boa noção de políticas de segurança e requerimentos aplicados para o sistema que eles gerenciam),

Administradores da área de sistemas e de Segurança da Informação (que detém bastante conhecimento técnico e tem um alto grau de autoridade nesse assunto), e os Gestores Operacionais junto com os Usuários do Sistema, que precisam se aprofundar sobre os conhecimentos de segurança para conduzir suas operações de trabalho.

Algumas perguntas-chave seriam interessantes de serem respondidas na criação desse material, como:

Que sensibilização, formação e/ou educação são necessárias?

O que está a ser feito atualmente para responder a estas necessidades?

Qual é a situação atual sobre a forma como estas necessidades estão sendo abordadas (ou seja, até que ponto os esforços estão funcionando)?

Quais as lacunas das necessidades e o que está sendo feito para resolvê-las?

Quais são as necessidades mais críticas?

É preciso pesquisar quais conhecimentos de segurança a equipe precisa e denota desconhecimento sobre, e há várias formas de coletar essa informação, aqui está uma sugestão de técnicas:

Entrevistas com todos os grupos e organizações-chave identificadas;

Pesquisas Organizacionais;

Revisar e avaliar recursos materiais disponíveis, como material de conscientização e formação atual, calendário e a lista de quem irá participar;

Analisar métricas que tem relação com a sensibilização e formação (exemplo: Porcentagem de pessoas que completam a sessão de conscientização necessárias, de acordo com o material específico da função);

Revisão do plano de segurança dos sistemas de apoio geral e aplicações para encontrar os proprietários dos sistemas e os representantes de segurança responsáveis;

Analisar o inventário do sistema e bases de dados de identificação de quem utiliza as aplicações para determinar os acessos;

Analisar as conclusões/recomendações de quem é responsável pela supervisão (Exemplo: Inquérito do Congresso, inspetor-geral, auditoria interna etc.) ou análise de programas relacionados ao programa de segurança da informação;

Conversas com a direção e proprietários do sistema, e o pessoal cuja execução do seu trabalho depende da TI;

Analisar eventos (como ataque DDoS – Ataque de Negação de Serviço, alteração de sites, sequestros de sistemas, ataques de malware etc.) pode ajudar a verificar o nível de conhecimento dos colaboradores e se precisa de formação, e quais grupos específicos precisam;

Revisar quando são efetuadas alterações técnicas ou de infraestrutura;

Estudar as tendências vistas em publicações acadêmicas ou governamentais, além como a utilização desses "Sistemas de alerta precoces", que pode identificar um problema na empresa que ainda não foi visto em primeiro momento.

A pergunta que precisa ser feita ao montar o material de treinamento é: "O que é que queremos que todo o pessoal da empresa saiba sobre a segurança da informação?" e "Quais habilidades gostaria que minha equipe aprendesse?". Além disso, é preciso que o treinamento seja sequenciado por uma lista de tópicos, dentre eles:

Utilização e gestão de senhas - como criação, alterações e proteção;

Proteção contra vírus, worms, cavalos de Troia e outros códigos maliciosos;

Política atualizada da empresa e suas implicações do não cumprimento, bem como os procedimentos que serão tomados para proteger a empresa contra um ciberataque e o contato técnico para assistência do funcionário;

Não abrir e-mails/anexos desconhecidos;

Utilização da Web, o que é permitido, o que é proibido na empresa, e monitoração do usuário do sistema;

O que é Spam e seus efeitos

Como fazer backup e armazenamento de dados (centralizada ou descentralizada);

Como se prevenir a engenharia social;

Como responder a incidentes, o que o funcionário pode fazer e quem ele deve procurar nesses casos;

O que o funcionário pode fazer caso esteja em acesso remoto ou home office

Alterações no ambiente e o que pode implicar de risco para os sistemas utilizados, como água, fogo, poeira etc.);

Inventário e transferência de propriedade, como identificar quem é responsável e qual é a responsabilidade dos funcionários, como a higienização de ferramentas de trabalho;

Diferenciação do uso profissional e pessoal dos dados e suas questões, bem como a segurança dos dispositivos de trabalho portáteis, bem como a segurança deles nas deslocações;

Softwares permitidos e suportados, quais deles tem restrições de licenças, quando são permitidas e não permitidas cópias, seus direitos de autor em relação a aplicativos pessoais no trabalho;

Questões de controle de acesso e abordagem do Princípio do Menor Privilégio, e separar tarefas;

Explicar o que é responsabilidade individual;

Utilização de declarações de acessos a sistemas e utilização;

Controle dos visitantes e de acesso físico aos espaços, para evitar vazões de informações confidenciais (no caso de um Tailgating, por exemplo);

Segurança do ambiente de trabalho, por exemplo, usar protetores de ecrã, restringir a visualização de informações para visitante no ecrã, gerenciar quem realmente irá ter acesso autorizado aos sistemas;

Proteger informação sujeita a preocupações de confidencialidades e que podem comprometer a empresa se forem vazados.

Aqui está um modelo com os tópicos que podem ser usados para montar o treinamento, só que traduzido em português e adaptado para a realidade brasileira. Também terá a lei e normas correspondentes do Brasil e dos Estados Unidos, mas caso não prefira fazer um curso internacional ou sua empresa não tem filiais no exterior, e caso nem tenha intenção de criar filiais em outros países, pode adaptar ao seu modo e utilizar apenas as normas brasileiras.

| **APÊNDICE A - Modelo de Plano do Programa de Formação e Sensibilização em Cibersegurança Empresarial** |
| --- |
| **RESUMO EXECUTIVO** |

**ANTECEDENTES**

Lei Geral de Proteção de Dados (LGPD), Estratégia de Governança Digital (EGD), Decreto nº 9.637/2018 - Política Nacional de Segurança da Informação, Estratégia Nacional de Segurança Cibernética (E-Ciber), Instrução Normativa nº1/DSIC/GSIPR ou a OMB A-130 Apêndice III.

Política específica do departamento e/ou agência (E outros fundamentos que podem ser relevantes dentro do programa de formação e sensibilização).

**POLÍTICA DE SEGURANÇA DA EMPRESA**

Metas;

Objetivos;

Funções e responsabilidades.

**CONSCIENTIZAÇÃO**

Público (gerência e todos os funcionários);

Atividades e datas previstas

Calendário

Revisão e atualização de materiais e métodos

**FORMAÇÃO E EDUCAÇÃO**

**Função 1: Executivos e Gestores**

- Objetivos de aprendizagem;
- Áreas de enfoque;
- Métodos/Atividades;
- Calendário;
- Critérios de avaliação.
- **Função 2: Área de segurança de TI**
- Objetivos de aprendizagem;
- Áreas de incidência;
- Métodos/Atividades;
- Calendário;
- Critérios de avaliação.
- **Função 3: Administradores de sistemas/redes**
- Objetivos de aprendizagem;
- Áreas de enfoque;
- Métodos/Atividades;
- Calendário;
- Critérios de avaliação.

...E outras funções responsabilidades significativas com a Segurança da Informação da empresa.

**CERTIFICAÇÃO PROFISSIONAL**

**Função 1: Para a área de segurança da informação**

- Objetivos de aprendizagem;
- Áreas de concentração;
- Métodos/Atividades;
- Calendário;
- Critérios de avaliação.
- **Função 2: Administradores de sistemas/redes**
- Objetivos de aprendizagem
- Áreas de foco
- Métodos/Atividades
- Cronograma
- Critérios de avaliação

...E outras funções responsabilidades significativas com a Segurança da Informação da empresa.

| **RECURSOS NECESSÁRIOS** | **CUSTOS** |
|---|---|
| Treinamento da equipe | **$ xxx** |
| Contratação de Suporte | **$ xxx** |
| Instalações (por exemplo, salas de | |

| | |
|---|---|
| formação)<br><br>Meios de comunicação (por exemplo, servidor(es) para material na Web e em computador) | **$ xxx**<br><br>**$ xxx** |

Uma vez finalizada o plano de formação em cibersegurança, os processos para estabelecer prioridades devem ser estabelecidos em um calendário de priorização, decidindo quais fatores utilizar e em qual sequência será continuado. Esses são:

Disponibilidade de material - é preciso considerar se os recursos para a produção do material estão disponíveis ou não, se há instrutores, entre outros;

Função e impacto organizacional – prioridade em termos de função e risco organizacional, e qual é a prioridade da empresa mediante ao seu histórico de prevenções e conhecimento dos funcionários;

Estado de conformidade atual – analisar as lacunas no programa de treinamento que podem ser melhoradas e qual é a fraqueza dos funcionários para implementar o treinamento antecipadamente;

Dependências do projeto – se há projetos que dependam de um segmento de formação de segurança no treinamento para preparar os requisitos necessários para o sistema (exemplo: treinamento de firewalls, VPNs, sistemas operativos etc.);

Para que uma técnica para realizar o treinamento seja efetiva, é preciso se atentar a quatro fatores:

Fácil de usar, de atualizar e manter;

O conteúdo pode ser usado para vários tipos de audiência em várias localidades;

Responsabilidade, como usar estatísticas da empresa para montar a conclusão;

Base considerável de apoio da indústria, como melhores hipóteses de encontrar apoio.

Há vários modelos que podem ser usados para mostrar o treinamento, como vídeos interativos para os funcionários, formação em plataformas web, formação presencial com interações entre instrutores e alunos, ou formação no site com o instrutor fazendo apresentações e mentorias.

### 2.2.2 Política de Privacidade, Controle de Acesso e *STIGs*

Normas, diretrizes e medidas de segurança pré-estabelecidas numa empresa podem ajudar a evitar possíveis e futuras invasões, além de revelar falhas no sistema de infraestrutura atual vigente. Além disso, faz-se importante estar em conformidade com as leis vigentes, como a Lei Geral de Proteção de Dados (LGPD), lei que por sua vez, assegura as boas práticas de governança e a segurança de clientes e parceiros. Mediante a isso, é importante destacar o uso das *Security Technical Implementation Guides (STIGs)* no campo da privacidade e controle de acesso, e um deles é o princípio do menor privilégio. Aqui estão algumas STIGs que merecem menção:

**Princípio do Menor Privilégio**

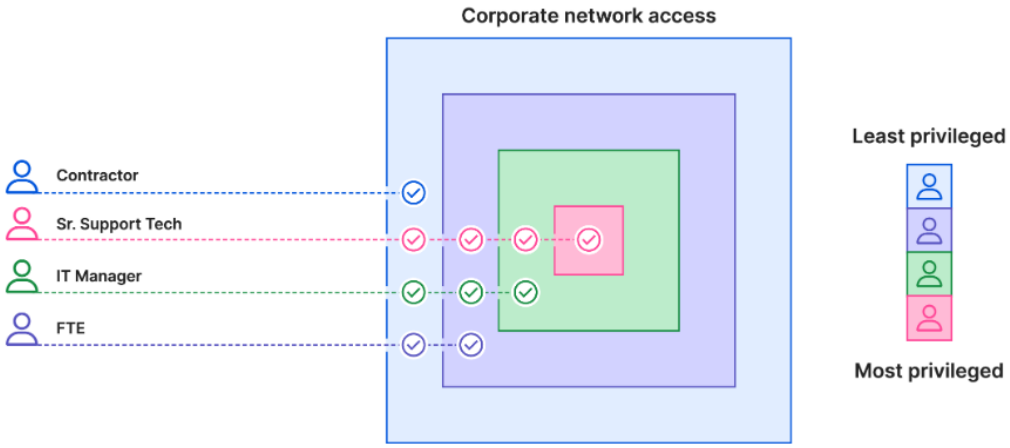



Figura 8. Figura mais simplificada, envolvendo quatro cargos, e suas permissões de acesso ao sistema, caracterizando o princípio do menor privilégio. Repare que, exceto o Técnico de Suporte Sênior, nenhum dos outros cargos tem acesso a todo o sistema (CLOUDFLARE, 2024).

Todos os usuários do sistema, até mesmo funcionários e administradores de alto escalão, tem permissões apenas para administrar no sistema o trabalho que lhes foi atribuído, sendo assim, nenhum deles tem domínio completo no sistema, e com isso, evita abusos, danos por parte de funcionários, ações de insiders ou whistleblowers e possíveis ataques futuros de Tailgating e de coleta massiva de dados por parte de hackers externos que invadem contas de funcionários. Também é popularmente conhecido como conhecimento dividido (STEWART; KINSEY; 2020).

**Gerenciamento de Vulnerabilidades**

Identifica e corrige falhas e vulnerabilidades em sistemas. Aborda sobre a implementação de patches de segurança e atualizações, de forma sistemática, para diminuir riscos de ataques futuros. A aplicação constante de correções é uma boa prática de segurança numa empresa. Há 3 técnicas que podem ser utilizadas para gerenciar os patches, sendo:

**Baseado em agentes:** Requer que um agente esteja sendo executado em cada sistema a ser corrigido, com um ou mais servidores que gerem o processo de

aplicação de patches e que seja coordenado com os agentes. Cada agente toma a responsabilidade de determinar qual software com vulnerabilidades está instalado no sistema, informar a equipe de servidores que gerencia os patches, pedir que novos patches sejam adicionados etc. Cada agente tem privilégios de administrador para que possam fazer essa monitoria. Esse método é recomendável para donos de sistemas que não estão na rede local a todo momento.

**Varredura sem agente:** É feita sem agente e é uma tecnologia que gere patches, com acesso administrador, que tem um ou mais servidores, que fazem a varredura de cada host que precisa ser corrigido e quais patches cada uma precisa. A principal vantagem é que não precisa ter agentes disponíveis para fazer a execução em cada host, tudo é feito automaticamente. Porém, em contrapartida, tem como ponto negativo não realizar a mudança e a monitoria para hosts que trabalham home office, ou que usam dispositivos móveis, além da possibilidade de não ser compatível com todos os softwares da organização.

**Monitoramento Passivo de Rede:** Também é feita por um programa, mas monitoram a rede local e digitalizam similar ao baseado em agentes, só que realizado por um programa, também não necessariamente precisa de privilégios locais, e podem ser usadas para monitorar os patches que a organização não controla, como sistema de visitantes e terceiros. A desvantagem é que só é possível usar em softwares em que possa identificar a versão baseado em seu tráfego de rede, e só funciona com hosts que trabalham presencialmente. (SCARFONE, Karen; SOUPPAYA, Murugiah, 2013).

Concomitante ao gerenciamento de vulnerabilidades, há duas STIGs que complementam este subcapitulo. São o Controle de Acesso STIG (*Access Control STIG*), que abordam autenticação de MFA, Auditoria e Monitoramento e a importância de ter uma base sólida de treinamento com a equipe, em concordância com a *NIST* (DISA, 2021), e a segunda é o STIG de Auditoria e responsabilização (*Audit and Accountability STIG*), que enfatiza a essencialidade de registrar eventos significativos que ocorrem nos sistemas (*Logging*), Monitoramento e Análise de Logs, Auditorias Regulares, Treinamento com os usuários e Proteção de Dados de Auditoria.

**Segurança de e-mails**

Muito eficaz para prevenir phishing e spear phishing. Lida com políticas de segurança para e-mails, usando diretrizes para esse fim. Uma das medidas recomendadas nessa STIG é a Autenticação Multifator (MFA), que garante que somente usuários autorizados terão acesso a e-mails, outra medida é o filtro de spam avançado, para bloquear e-mails duvidosos antes de chegar na caixa de e-mail dos usuários. A implementação de políticas rigorosas de e-mail e a educação dos usuários na cibersegurança básica, se tornam cruciais para minimizar ataques de engenharia social. (DEFENSE INFORMATION SYSTEMS AGENCY, 2024). A *ISO/IEC 27002* (2022) também recomenda fortemente o uso criptografia de ponta a ponta e monitoramento de tráfego de e-mails. Abaixo, terão dois guias técnicos da STIG do qual vale a pena menção:

**Guia de Implementação Técnica de Segurança do Microsoft Outlook 2016** ***(Microsoft Outlook 2016 Security Technical Implementation Guide)***

No ID V-228465 desse guia, há uma recomendação de que os hiperlinks em mensagens de e-mail suspeitas de phishing devem ser proibidos, ou seja, a política vigente estabelecida ordena que não se podem fazer hiperligações em e-mails suspeitas de phishing no Outlook. Se ativar os hiperlinks, o Outlook permitirá hiperligação nesses e-mails suspeitos.

Em ID V-228464, informa-se para habilitar o aviso sobre macros não confiáveis no Outlook, correspondente ao "Aviso para todos os macros" na seção "Segurança Macro" da Central de Confiabilidade, sendo assim, subsequentemente,

No ID V-228466, destaca-se que a Criptografia RPC entre o Outlook e o Exchange Server deve ser ativada. Paralelo a isso, o ID V-228467 tem uma conduta similar, ele recomenda que o Outlook deve ser configurado para forçar a autenticação ao se conectar a um servidor Exchange.

**STIGS de Políticas de Serviço de E-mails**

O ID V-18877 determina que os grupos de administradores de e-mail da empresa devem garantir o menor privilégio, e em relação a sua função, o ID V-18869 integra que é fortemente recomendado trilhas de auditoria de e-mail, e que é interessante que sejam feitas revisões diariamente. Além disso, é importante que os registros de auditoria sejam mantidos por 1 ano, segundo o ID V-18879. A pesquisa e a auditoria se tornam importantes pois pode ter ações maliciosas que podem ter acontecido e arquitetadas antes da auditoria.

Entretanto, no ID V-18867, ressalta que os Serviços de E-mail devem ser documentados no EDSP (Plano de Segurança de Domínio de E-mail). Relacionado, há o ID V-18885, que complementa que a política de uso aceitável de e-mail deve ser documentada no Plano de Segurança de domínio de e-mail. Outras IDs que valem a pena destacar o ID V-33389, em que a política de uso aceitável de e-mail deve ser renovada anualmente, e V-18886, em que a Política de Uso Aceitável por Email deve conter os elementos necessários, isto é, educação e expectativas do usuário, e penalidades do não cumprimento, podendo obter classificação e rotulagem de sensibilidade, ensinar a reconhecer mensagens indesejadas ou suspeitas (SPAM, Phishing, etc.), ressaltando quais os serviços oficiais de e-mail (Outlook, Gmail, entre outros), cotas de tamanho da caixa de e-mail, limitar anexos e etapas para fazer solicitação de help ou service desk.

No ID V-18881, ressalta a importância de backups e recuperação de e-mail, e a importância de ser documentada e testada em uma frequência compatível com INFOCON e seus níveis, planos de recuperação e de desastres de instalações via e-mail.

**STIG de Segurança dos pontos terminais (*Endpoint Security STIG*)**

Ajuda na prevenção de Engenharias Sociais de forma geral, pois protege os pontos terminais com criptografia de ponta. Aborda a aplicação de patches, controle de proteção, bloqueio de scripts maliciosos e prevenção de execução de códigos externos e não autorizados. Os STIGS a se destacar são o Guia de Requisitos de Segurança do Servidor de Gerenciamento de Endpoint Unificado (Unified Endpoint Management Server Security Requirements Guide) e o STIG do Antivírus Windows Defender (Windows Defender Antivirus STIG).

**Guia de Requisitos de Segurança do Servidor de Gerenciamento de Endpoint Unificado (Unified Endpoint Management Server Security Requirements Guide):**

No ID V-234668, cita a importância de mecanismos de proteção de confidencialidade. Ele alega que O servidor UEM deve ser configurado para implementar o modo FIPS 140-2 para toda a criptografia de servidor e agente. Sem esses mecanismos, pessoas não autorizadas podem obter acesso a informações confidenciais por meio de acesso remoto, que, por sua vez, o acesso remoto é o sistema de informações por um usuário autorizado, que se conecta fora da rede da organização (Exemplo: Home Office). Para que a implementação seja feita, e seja listada pelo certificado do modo criptográfico FIPS 140-2 (uma norma do governo dos Estados Unidos e publicada pela *National Institute of Standards and Technology* (NIST) e define o mínimo de segurança criptográfica, em hardware, software e firmware), deve completar o processo de validação do algoritmo. Os módulos autorizados segundo a NIST são BCE, CBC, OFB, CFB, CTR, XTS-AES, FF1, FF3, CCM, GCM, KW, KWP e TKW. Paralelo a isso, no ID V- 234383, que complementa que o servidor UEM deve usar a função hash SHA-2 ou superior validada por FIPS para proteger a integridade do código de autenticação de mensagens hash com chave (HMAC), Funções de Derivação de Chave (KDFs), Geração de Bit Aleatória e aplicativos somente hash. Recomendações são SNMPv3, SSH, NTP, HMAC e KDFs. Envolve integridade do código de autenticação de mensagens (HMAC), usar as funções Derivação de Chave (KDFs) e Geração de Bit Aleatória.

**STIG do Antivírus Windows Defender (Windows Defender Antivirus STIG)**

O ID V-75153 alega que o Windows Defender AV deve ser configurado para executar e procurar malware e outros softwares potencialmente indesejados. Paralelamente, o V-75151 aborda que o Defender AV deve ser ajustado para executar automaticamente todas as tarefas detectadas e, juntamente, o ID V- 75225, o Defender deve ser colocado para verificar todos os arquivos e anexos baixados e para bloquear o conteúdo executável do cliente de e-mail e do webmail (V-77965).

Além das STIGs, outra coisa que deve se atentar são os controles de acesso. De acordo com ISO (2013), recomenda-se controles de acesso lógico e físico, e que o controle de acesso escolhido esteja em concordância com requisitos de segurança de negócios individuais, política de autorização da informação, níveis de segurança e classificações, concomitância entre direitos de acesso e políticas de classificação das informações, obrigação contratual com proteção de acesso de dados, gerenciar direitos de acesso, segregar direitos de acesso de acordo com a função, requisitos para pedir autorização de acesso, bem como análises críticas de direitos de acesso e regras, e registro de todos os eventos relacionadas a esse tipo de gerenciamento.

### 2.2.3 Autenticação Multifator (MFA)

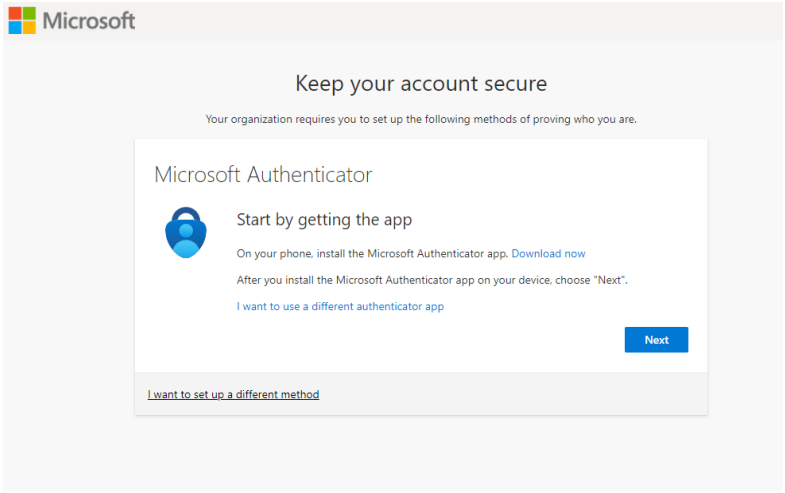



Figura 9. O Microsoft Authenticator é um exemplo de Software MFA popularmente utilizado.

De acordo com Kaufman et al. (2022), a autenticação e a verificação viável e fidedigna da identidade humana de alguém, enquanto a Autenticação Multifator é uma maneira mais segura, em que a pessoa se autentica utilizando mecanismos de várias categorias, um sistema de múltiplas camadas, como um código exibido na tela em que você precisa confirmar em um aplicativo de autenticação, ou um envio de código PIN para o celular do utilizador, eles também ressaltam que implementar MFA em sistemas corporativos fortalecem a segurança das credenciais, e são uma barreira contra fraudes e ameaças.

Segundo o National Institute of Standards and Technology (NIST), a Autenticação Multifator usa senhas, tokens físicos ou biometria. Complementando, conforme relatado pela Cybersecurity and Infrastructure Security Agency (CISA), a MFA reduz de forma relevante o risco de comprometer a conta, combinando algo que o usuário sabe – sua senha – algo que ele possui – token – e algo que o usuário é – biometria, e seu uso é fortemente recomendado em corporações, sistemas governamentais e militares.

### 2.2.4 Boas Práticas de Descarte de Informações

Cuidar do descarte de informação é crucial para evitar *dumpster diving*. Caso não realize esses procedimentos, aumentam consideravelmente os riscos de acessos não autorizados, ataques de engenharia social, expondo informações confidenciais. Conforme ISO (2013), há algumas diretrizes para descarte de mídias, sendo:

> Mídias contendo informações confidenciais sejam guardadas e destruídas de forma segura, por incineração ou trituração, ou remoção de dados.
>
> É necessário que tenha uma vistoria prévia para verificar os itens que precisam de descarte seguro.

> É interessante separar as mídias que serão inutilizadas de forma geral e descartá-las, ao invés de apenas descartar as confidenciais.
>
> Algumas empresas oferecem serviços de descarte, porém, esteja atento e informado ao selecionar um fornecedor, ele precisará ter experiência e controle apropriado.
>
> Toda vez que for descartar uma informação sensível, registre, para manter uma auditoria consistente.

Agora, iremos detalhar os procedimentos e citar alguns que são citados academicamente, mas não foram citados pela ISO.

**Descarte de documentos físicos**

Para documentos de informações confidenciais, o melhor método é usar triturador de papel. Segundo Stamp (2014), a destruição é uma boa prática de confidencialidade, em destaque para informações PII (Personally Identifiable Information, ou Informações Pessoais Identificáveis).

Queima controlável: Para documentos que não podem ser reciclados e são muito sensíveis (Kaufman et al, 2022).

Armazenamento Seguro até Descarte: Um bom método para que o conteúdo não seja acessado antes do descarte, onde só podem ser acessadas por pessoas autorizadas.

**Descarte para dados digitais**

Sobrescrita de dados: Usar ferramentas que sobrescrevem dados no disco rígido várias vezes, impossibilitando a visualização do conteúdo anterior (NIST, 2014).

Desmagnetismo: Aplica um campo magnético que desmagnetiza o hardware, como discos, sendo impossível de recuperar (Miller et al., 2010)

Destruição física do Hardware: Se o conteúdo está em disco rígido e não foi postado na web, esmagar o disco rígido ou o hardware de armazenamento também é um método viável.

Segundo Long (2008), há milímetros e tipos de cortes recomendados para cada documento:

| Tipo | Tamanho do corte | Propósito |
|---|---|---|
| Corte em tiras | 0,95 cm | Documentos gerais |

| | | |
|---|---|---|
| Corte transversal | 0,95 cm x 3,81 cm - 8,57cm | Documentos gerais |
| Corte em tiras | 0,63 cm - 0,31 cm | Documentos sensíveis |
| Corte em tiras | 0,15 cm | Documentos confidenciais |
| Corte transversal | 0,31 x 1 - 0,31cm | Documentos confidenciais |
| Corte transversal | 0,158cm x 1,58cm | Documentos Secretos |
| Corte transversal | 0,07cm x 1,27cm | Documentos “Top Secrets”, ou seja, documentos secretos governamentais |
| Corte transversal | 1mm x 5mm | Documento de alta segurança governamental |

### 2.2.5 Resposta a Incidentes, Recuperação e Análise Pós-Incidente

É um conjunto de ações para mitigar o impacto de uma segurança violada dentro da empresa. É preciso testar periodicamente as respostas, para que, quando acontecer o incidente, a resposta seja eficaz. Lidar com incidentes envolve mais do que aplicar procedimentos básicos – precisa de agilidade, coordenação e equipe preparada para responder de maneira rápida e eficiente (STAMP, 2022). Conforme NIST SP 800-61r2 (2012), é recomendável que uma equipe de resposta a esses problemas seja criada, ou como eles nomeiam, *Computer Security Incident Response Team* (CSIRT) – Equipe de Resposta a Incidente de Segurança na Informática. Possíveis prevenções são:

- Teste de penetração: Realizar simulações de ataques para verificar vulnerabilidades no sistema e corrigi-los.

- Implementação de Firewalls e IDS/IPS: É sempre positivo colocar sistemas de detecção, para monitorar o tráfego de rede e alertar sobre invasões ou atividades suspeitas, facilitando na identificação quando ocorrer e possibilitando responder mais rapidamente.

**Resposta a Incidentes:**

**Contê-lo**: É estritamente necessário que se contenha o incidente, para que ele não se espalhe pelo sistema da empresa. A contenção pode ser desconexão temporária de redes comprometidas, a desativação de serviços críticos ou o bloqueio de usuários suspeitos. Em vazamento de dados, o essencial é limitar o alcance, segundo as diretrizes de resposta a incidentes do *NIST* (Scarfone; Souppaya, 2013). Outra coisa que pode ser feita é separar os servidores comprometidos, para que não atinja outros servidores da empresa. Alguns exemplos de software que podem ser usados serão abordados no subcapítulo “Uso de Tecnologias e Ferramentas de Segurança”. Outras formas também que ajudam a mitigar é suspensão temporária de acesso da conta invadida ou verificação de senha dessas contas.

**Documentação Rigorosa**: Durante todo o processo de resposta, a equipe tem que documentar cada medida que foi tomada. Killmeyer (2006) defende que, ao fazer isso, a equipe tem uma análise mais completa que pode ser revista e auditada posteriormente, caso aconteça novamente algum incidente parecido, bem como servir como uma base de conhecimento. Segundo *NIST* (2012), é recomendado que essa documentação de incidente tenha:

- O estado atual do incidente (novo, em curso, encaminhado para investigação, resolvido...);

- Resumo do incidente;

- Indicadores relacionados com o incidente;

- Outros incidentes relacionados (se houver);

- Ações tomadas por todos os responsáveis pelo incidente em relação a este incidente;

- Cadeia de custódia (caso houve);

- Avaliações de impacto relacionadas com o incidente

- Informações de contato de outras partes (por exemplo, no meio do incidente, conversaram com proprietários de sistemas, administradores de sistemas...);

- Uma lista de provas recolhidas durante a investigação;

- Comentários dos responsáveis pelo incidente (se for interno);

- Próximas medidas a serem tomadas;

**Recuperação:**

O próximo passo depois da contenção é a recuperação. Conforme Anderson (2019), envolve restaurar os serviços e validar que a ameaça foi expurgada antes de reativar. Alguns procedimentos são:

**Reinstalar os sistemas**: Em casos extremos, e depois de verificar que o invasor não está mais no sistema, o recomendado é que se reinstale os programas ou restaure-os por backup. Segundo Killmeyer (2020), restaurar por backups reduz a chance de reintroduzir a ameaça.

**Verificar Integridade**: Antes de restaurar os softwares usados, é preciso fazer verificações as contas ou o alvo que foi invadido anteriormente esteja sem ameaças e seguro. *NIST* (2012) sugere que uso de ferramentas de integridade ajuda a garantir que está seguro e protegido antes de voltar a ser acessado por funcionários. Algumas são os aplicativos Tripwire, OSSEC, Veracode, HashCalc, entre outras.

### 2.2.6 Uso de Tecnologia e Ferramentas de Segurança

Para ajudar na prevenção e mitigação descritas anteriormente, existem vários softwares que podem fornecer uma resposta aos incidentes ou prevenção. Aqui estão alguns a se levar em consideração:

**Conscientização dos Usuários**:

**Sophos Phish Threat:** Um software que dá treinamentos sobre phishing em português, que também tem simulações de ataques dentro da plataforma para que os usuários possam identificar a veracidade nos exercícios. Essa ferramenta é paga, mas tem um teste grátis de 30 dias.

**Política de Privacidade, Controle de Acesso e STIGs**:

**ManageEngine ADManager Plus:** Um software para controle de acesso e gerenciamento de privilégios usando o método de Active Directory.

**Microsoft Azure AD:** Também é uma plataforma de gerenciamento de identidades e acesso, atendendo também as STIGs citados.

**Autenticação Multifator**

**Microsoft Authenticator:** oferece autenticação multifator (MFA) para sistemas.

**Google Authenticator:** Concorrente do Microsoft Authenticator, também oferece autenticação multifator (MFA), e é uma boa alternativa.

**Boas Práticas de Descarte de Informações**

**CCleaner:** Auxilia no descarte de dados, removendo informações e limpar arquivos temporários.

**Resposta a Incidentes, Recuperação e Análise pós-incidente**

**Kaspersky Endpoint Security:** Uma ferramenta que ajuda nas respostas a incidentes, podendo bloquear ameaça e recuperar arquivos posteriormente, diminuindo propagação e ajuda no análise pós-incidente.

**SolarWinds Security Event Manager:** Uma plataforma que monitora e responde a incidentes com log de eventos em tempo real, facilitando também a análise de incidentes.

Sem contar com Tripwire, OSSEC, Veracode e HashCalc já citadas anteriormente.

**Ferramentas para proteger o computador dos funcionários**

**Avast Business Antivirus:** ajuda a identificar monitoramento de dispositivos e faz varredura de ameaças.

**BitDefender GravityZone**: fornece soluções de prevenção contra malware, ransomware e outros ataques.

### 2.2.7 Execução Ética

Para ficar mais prático de entender e inteligível dentro do texto, elaboramos alguns subcapítulos, para garantir a organização e a clareza. Lembrando que falaremos da Execução Ética, ou seja, aplicado mediante a permissão da empresa, respeitando as normas e leis vigentes, sem violar quaisquer direitos, protegendo a integridade das informações. Além disso, estará sobre o tema da Engenharia Social, portanto, não será apresentado algo fora desse tema ou que não seja relacionado.

Responsabilidade e Regulamentação;

Testes e Simulações Éticas;

### 2.2.8 Responsabilidade e Regulamentação;

No Brasil, é visível que há vários conjuntos de leis e normas que ditam e colocam diretrizes em relação a cibersegurança na Internet, e que todos os *pentesters* devem seguir, devido a essa fundamentação de diretrizes. A finalidade dessas normas são para combater

crimes cibernéticos, prevenir abusos e garantir que as ferramentas serão usadas de forma ética. Abaixo, estão as leis que tangem a ética da cibersegurança no Brasil:

**Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018)**

A LGPD é a base principal de proteção de dados no Brasil, e inspirada na GDPR da União Europeia. O objetivo é garantir privacidade de dados das pessoas clientes e compradores dentro das empresas, estabelecendo regras de uso e tratamento das informações dessas pessoas. Ele obriga as organizações a adotarem medidas técnicas e administrativas para evitar acessos não autorizados, dentre outros incidentes. Toda vez que tiver incidente de segurança, se faz necessário as empresas comunicarem rapidamente a Autoridade Nacional de Proteção de Dados (ANPD) e os afetados. As multas são:

> "*multa simples, de até 2% (dois por cento) do faturamento da **pessoa jurídica de direito privado**, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) **por infração** (BRASIL, 2018)".*

**Marco Civil da Internet (Lei nº 12.965/2014)**

O marco civil da Internet funciona como um código de conduta com um conjunto de direitos e deveres para empresas e usuários. Sua função envolve garantir a privacidade, em que os dados das pessoas só podem ser guardados mediante consentimento, as empresas são obrigadas por lei a proteger os dados dos usuários e exige esclarecimento em relação a como as empresas usam os dados coletados. Aqui estão alguns artigos importantes de ser= levar em consideração sendo um profissional da segurança da informação.

> *"Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.*
>
> *§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial [...].*
>
> *§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial [...].*
>
> *§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.*

> *§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais." (BRASIL, 2014).*

O não cumprimento resulta em multa de até 10% do faturamento do grupo econômico no Brasil no seu último exercício, excluídos tributos**.**

**Lei Carolina Dieckmann (12.737/2012)**

Nessa lei contra crimes cibernéticos, há um artigo que seria interessante fazer menção, que podem estar relacionados com o tema desse trabalho. Esse é o artigo 154-A:

> *"Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita".*

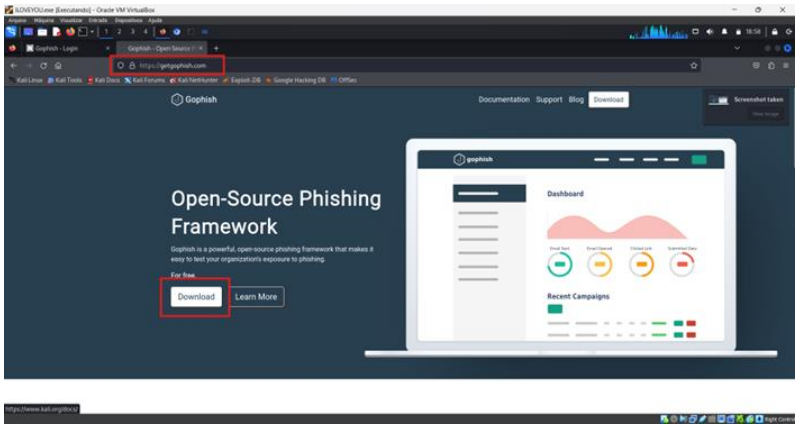
A pena é de detenção de 3 meses a 1 ano, e multa, que pode aumentar para 6 meses a 2 anos com multa se a invasão tiver a coleta de informações sigilosas e segredos comerciais".

### 2.2.9 Testes e simulações éticas

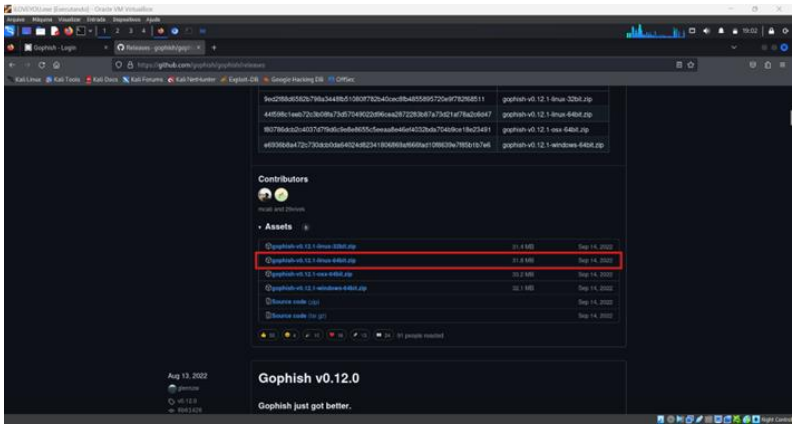
**Lembrando: Não use indevidamente para fins não éticos. O que é demonstrado abaixo é apenas para fins educativos.**

Há algumas ferramentas legais para se conhecer que podem ser usados para *pentest* ou em segurança ofensiva, portanto, iremos falar de cada uma delas, como fazer a instalação, e como manusear.

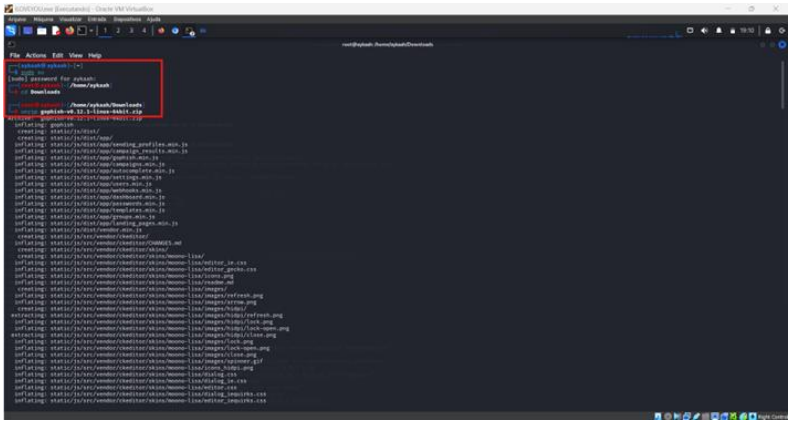
*GoPhish*: Primeiramente, vá em [https://getgophish.com](https://getgophish.com) e faça o *download*.



Após isso, iremos ser direcionados para uma página do *GitHub*, quando chegar lá, desça até o final com o scroll do mouse e clica em "*gophish-v0.12.1-linux-64bit.zip*", para *Linux* (Se for instalar no *Windows*, baixe o "*gophish-v0.12.1-windows-64bit.zip*");

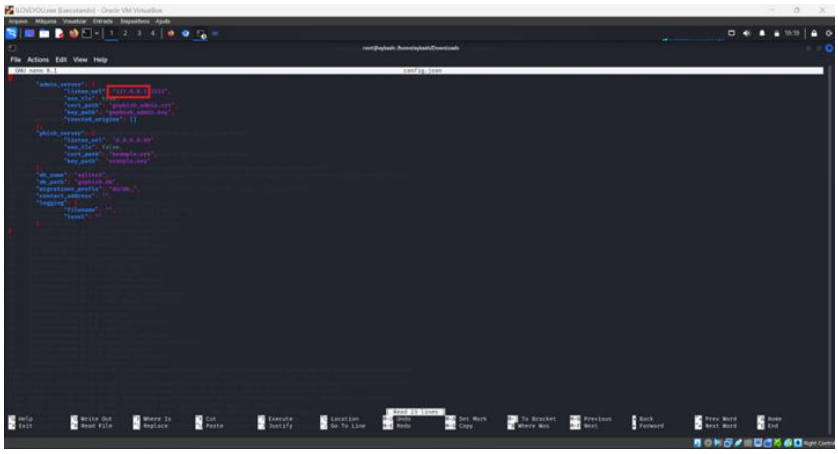



Ao baixar, vá em *Terminal Emulator* (Prompt de Comando), e siga esses procedimentos;

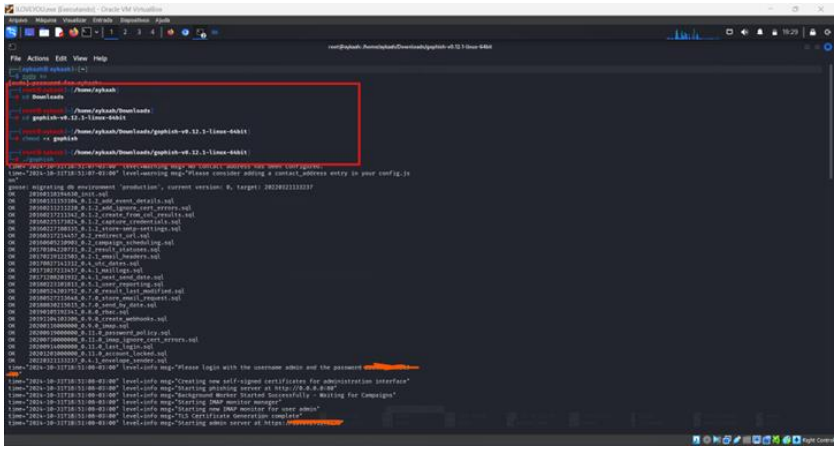


Depois, precisamos configurar o *config.json*. Para isso, precisamos saber o *IP* da nossa máquina, para descobrir, só digitar *hostname -I*. Após isso, e já com o *IP*, siga a imagem;

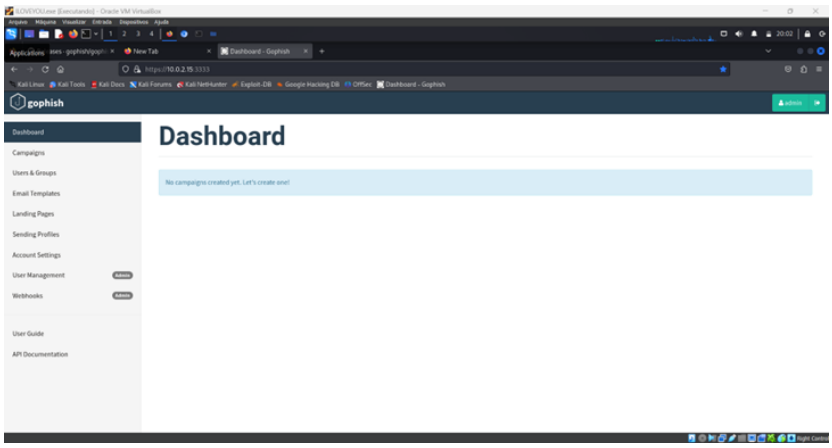
Vai abrir esse documento, no retângulo em vermelho, é onde precisa colocar o *IP*;



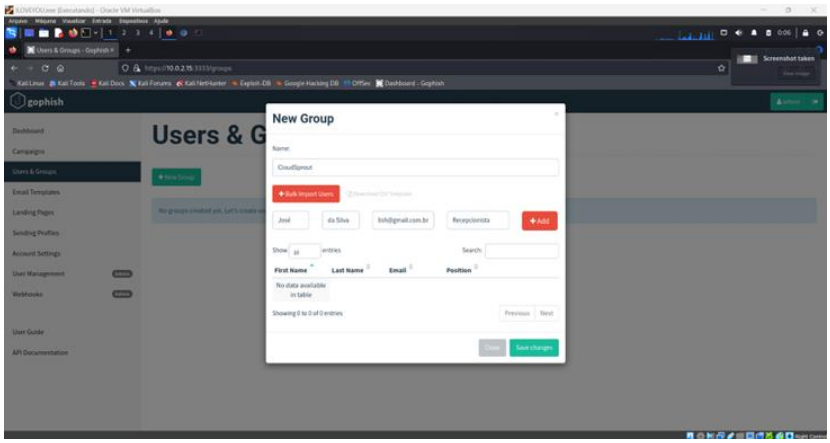
Para sair, clique em *CTRL+O* para salvar, *CTRL+X* para sair e volte ao *prompt*. Depois, precisamos dar permissões de administrador ao *GoPhish* e executar, siga o que está na imagem abaixo;



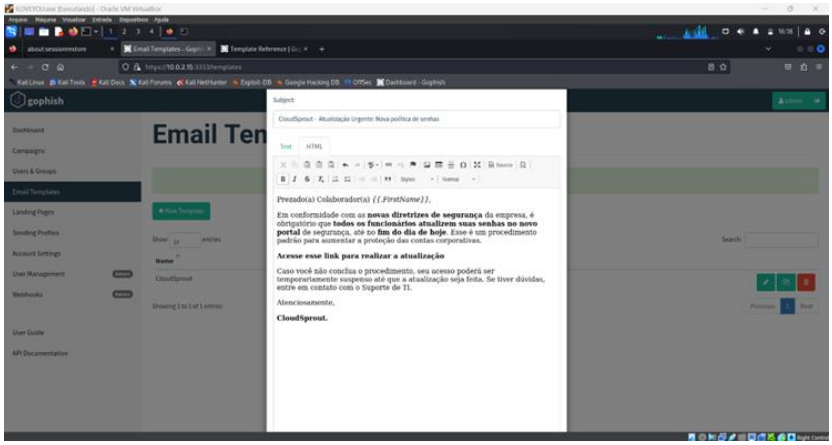
Terá um link no final do código, que é esse *level= info msg "Starting admin server at https://:000.000.000.00"* (seu *ID*). Sua senha estará em *level-info msg= "Please login with the username admin and the password* (senha autogerada)". Ao clicar no link com seu *ID*, irá abrir uma página na web com problema de certificado do *Firefox*, só clicar em "*Advanced*" e *"Accept the risks"*, e conectar no login do *GoPhish* com o usuário *"admin"* e a senha que foi oferecida.



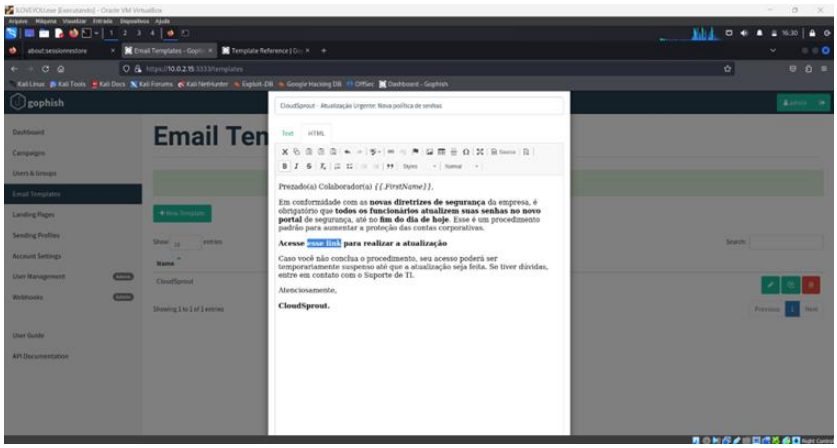
Vá em *Users & Groups* e clique em *New Group* para adicionar uma Corporação. No nosso caso, será uma empresa fictícia chamada *CloudSprout*. Adicionamos um José da Silva, e um e-mail onde é possível testar. Após isso, clica em *Add* e em seguida *Save Changes*.



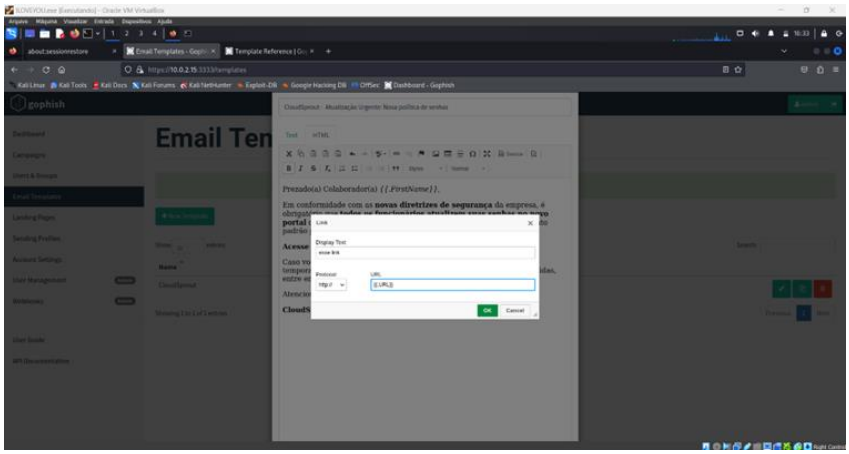

Em seguida, iremos elaborar nosso template de e-mail duvidoso para enviar para José da Silva. Clique em *Email Templates* na aba lateral e clicar depois num botão verde escrito *New Template*, e preencha o nome do *template*, e o título do *e-mail*, depois vai em *HTML*, *Source* na barra abaixo do *html* e escreva o *template* do corpo do *e-mail*, pode ser o que desejar, e se quiser pode anexar uma imagem em *Add Files*. Você também pode escrever seu e-mail usando as referenciações disponíveis nesse link [*https://docs.getgophish.com/user-guide/template-reference*](https://docs.getgophish.com/user-guide/template-reference). No exemplo, foi escrito dessa maneira:



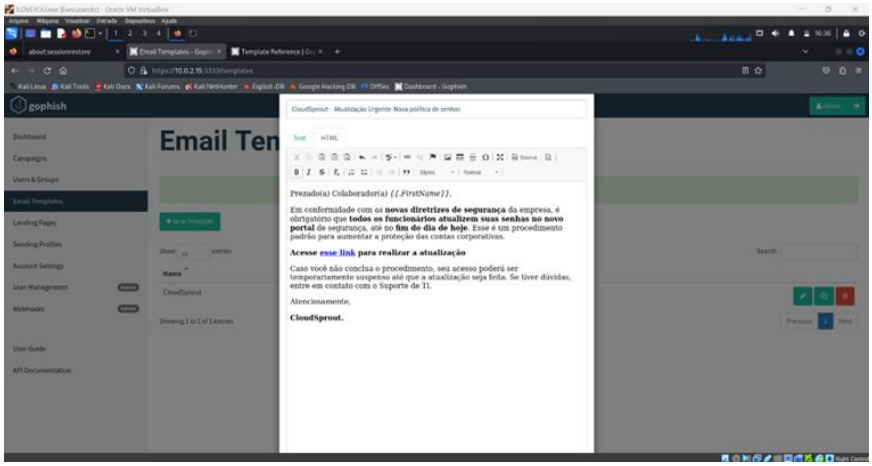

Agora, iremos colocar link em “esse *link*”. Passe o *mouse* m cima dessa frase e selecione.



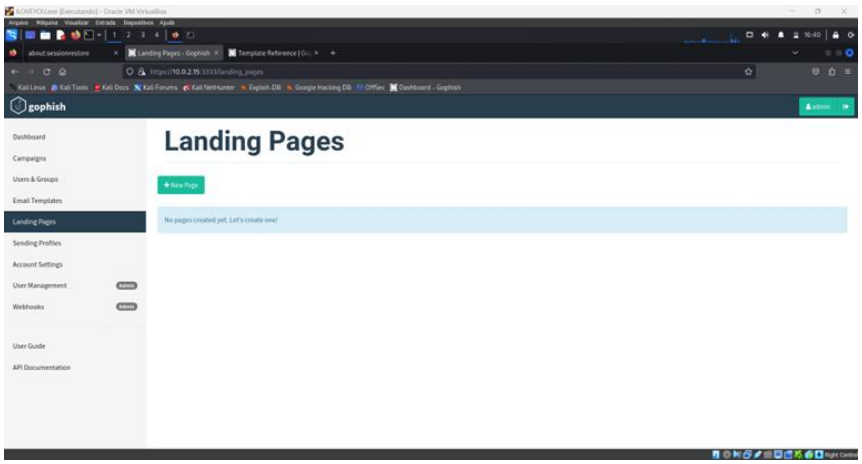
Em seguida, clique *CTRL+K* no teclado e digite dessa forma, depois clique em *OK*:



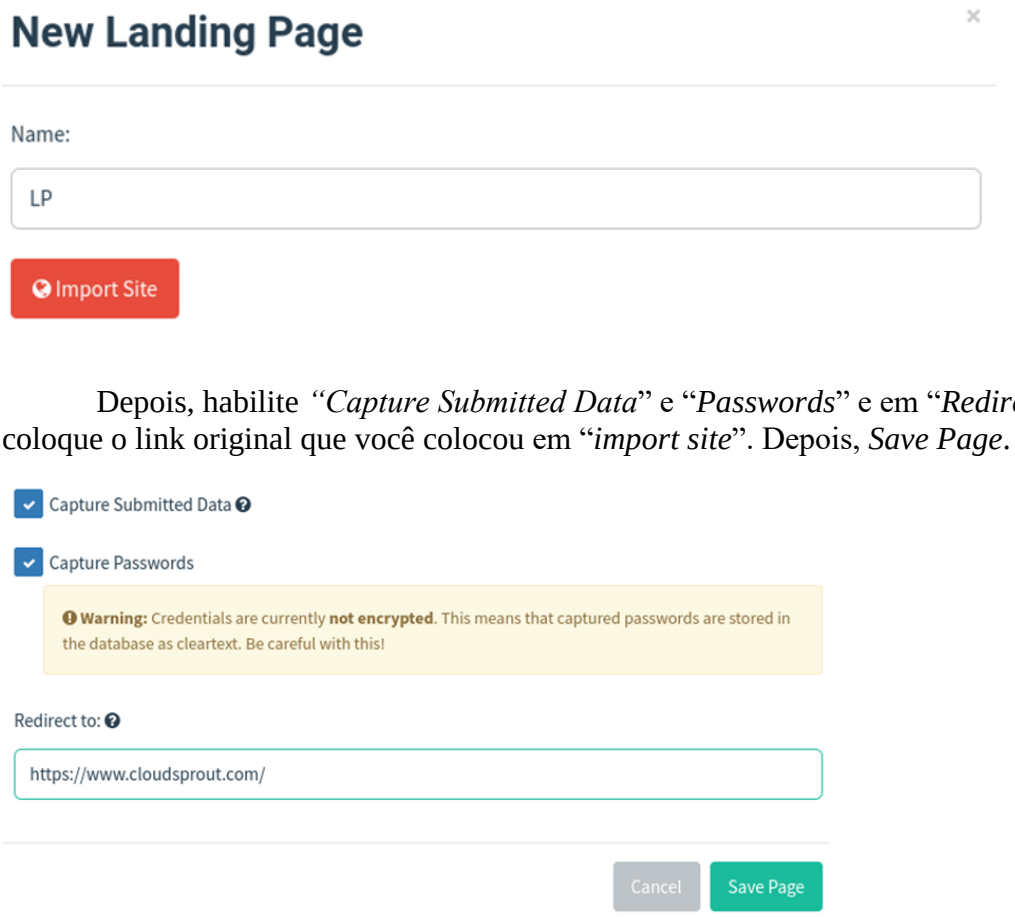
Pronto. Nosso link ficou no meio do *template* e as palavras ficaram sublinhadas e azuis. Clique em *Save Template.*



Agora vamos montar o link duvidoso. Vá em *Landing Pages* na aba lateral e em *New Pages.*



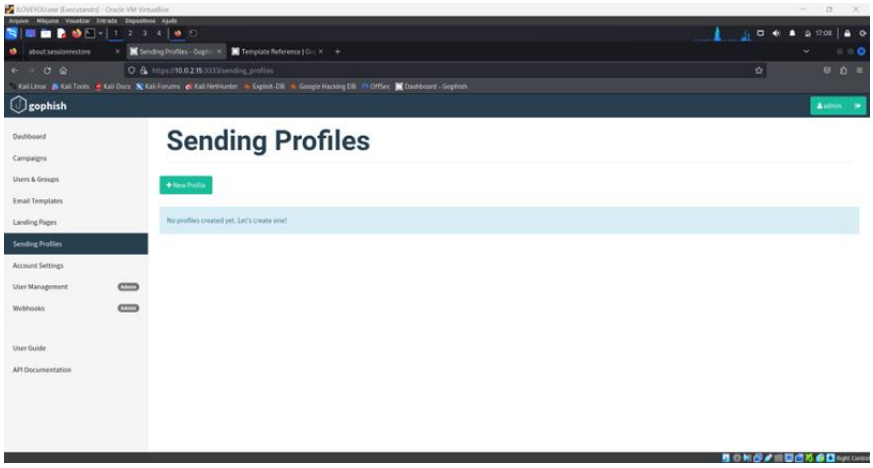
Depois, coloque o nome e o site que deseja ser clonado. O *GoPhish* faz todo o trabalho duro de clonar.



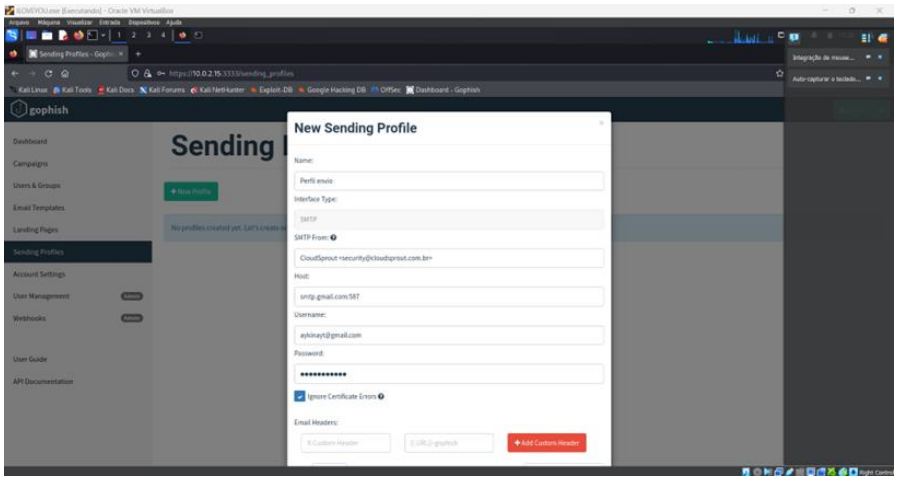

Depois, habilite *"Capture Submitted Data*" e "*Passwords*" e em "*Redirect to*", coloque o link original que você colocou em "*import site*". Depois, *Save Page*.



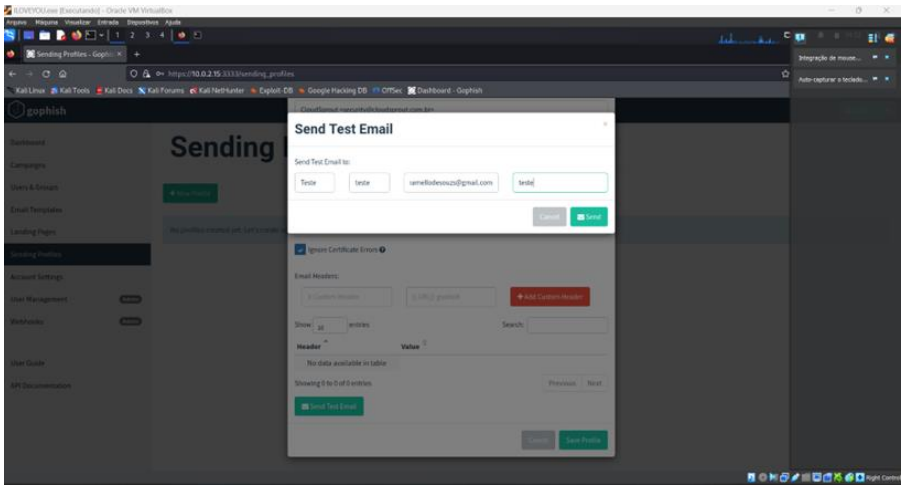

Agora vamos criar nosso usuário para enviar o e-mail, para que José da Silva não desconfie da origem do e-mail. Vá em *Sending Profiles* e depois em *New Profile*.



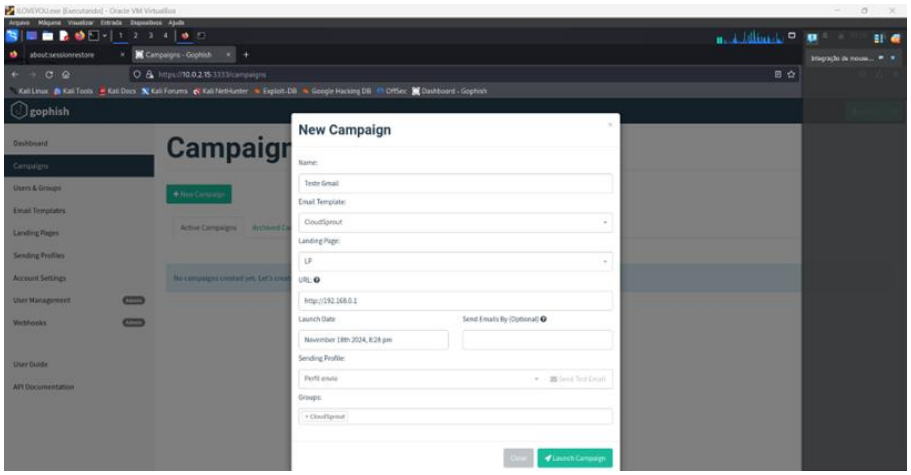

Depois, preencha as informações. Aqui, preenchemos dessa forma. O nome pode ser qualquer um de sua preferência, o SMTP From seria o nome do e-mail que vai enviar a mensagem.




Lembrando que a porta *SMTP* colocada é o padrão do *Gmail* devido a esse ser um teste fictício, mas em situações reais, com empresas, é usada a porta estabelecida pela empresa ou o domínio utilizado, para que a simulação fique mais realista. Em *Username*, coloquei meu e-mail de teste, que era outro e-mail do que foi utilizado para registrar José da Silva. Agora, vamos enviar um e-mail de teste antes de testar com José da Silva, para ver se o serviço de e-mail está funcionando. No *e-mail*, coloquei o que foi colocado em *Username.* Se o teste deu certo, clique em *Save Profile*.




Vamos ir para *Campaigns* agora e clicar em *New Campaign*. Escreva nome, selecione *template* do *e-mail*, *Landing Page* que será utilizada. No campo da *URL* tem que inserir no formato *http://<ip*>, pois, caso insire na forma *https*, quando a vítima tentar entrar no *link*, vai dar erro no carregamento.



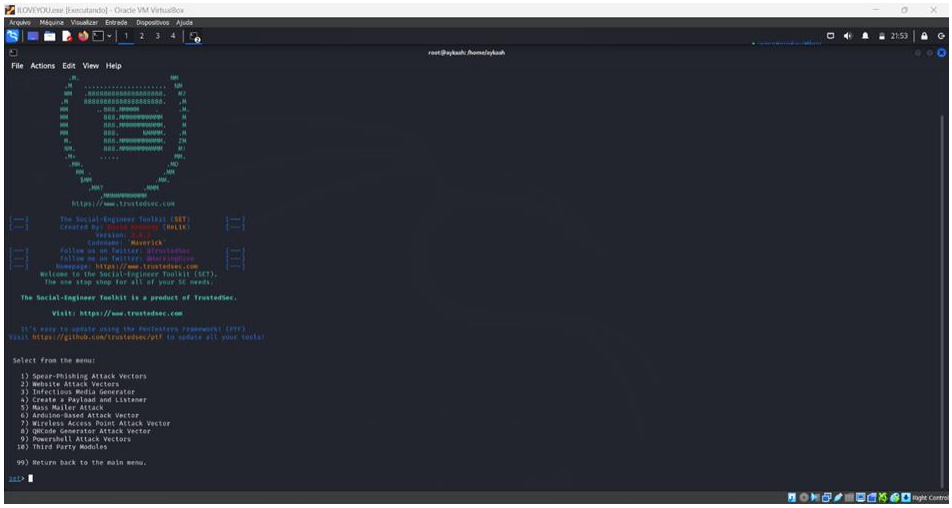

Quando a vítima cai no e-mail, é assim que aparece:



## SOCIAL ENGINEERING TOOLKIT

Nesse caso, iremos criar um clone de site já existente. Para realizá-lo, iremos clicar no *1) Social-Engineering Attacks*

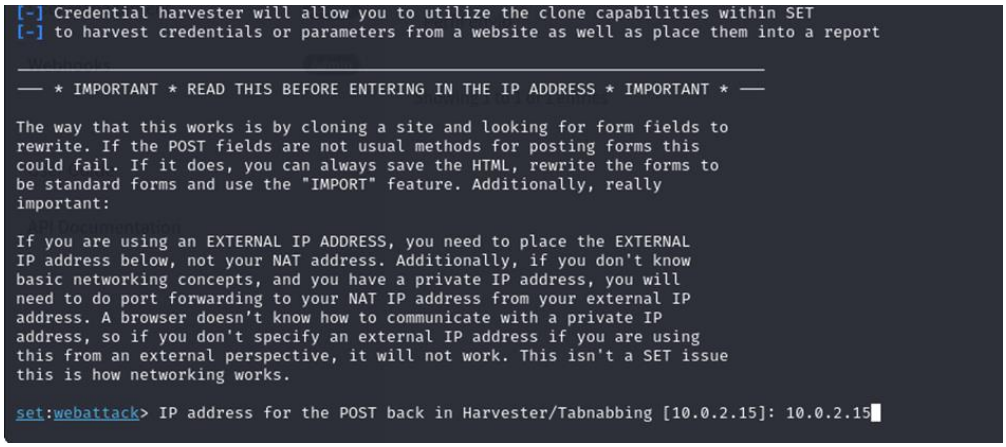

Dentro de Social-Engineering Attacks, aparecerá um outro menu. Clique em *2) Website Attack Vectors.*



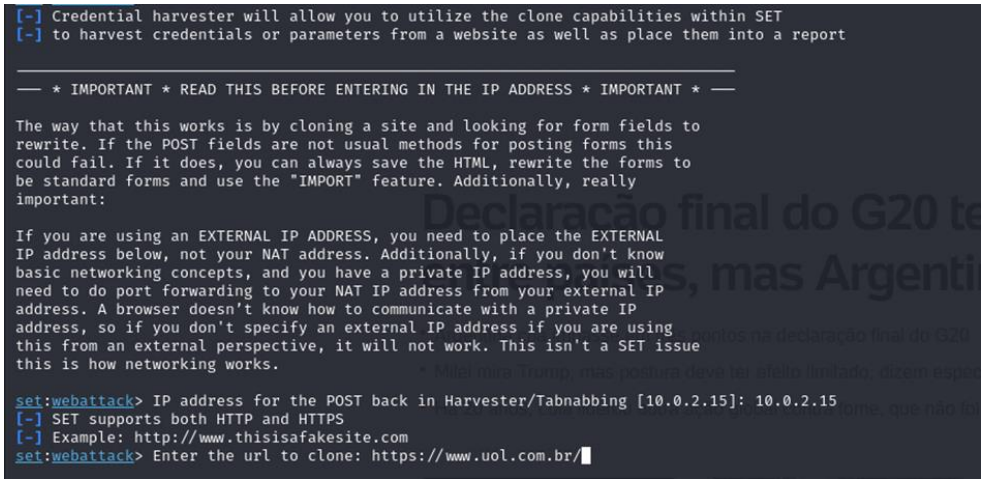

Depois, vá em *3) Credential Harvester Attack Method*:


Depois, irá aparecer outro menu. Escolha *2) Site Cloner*.

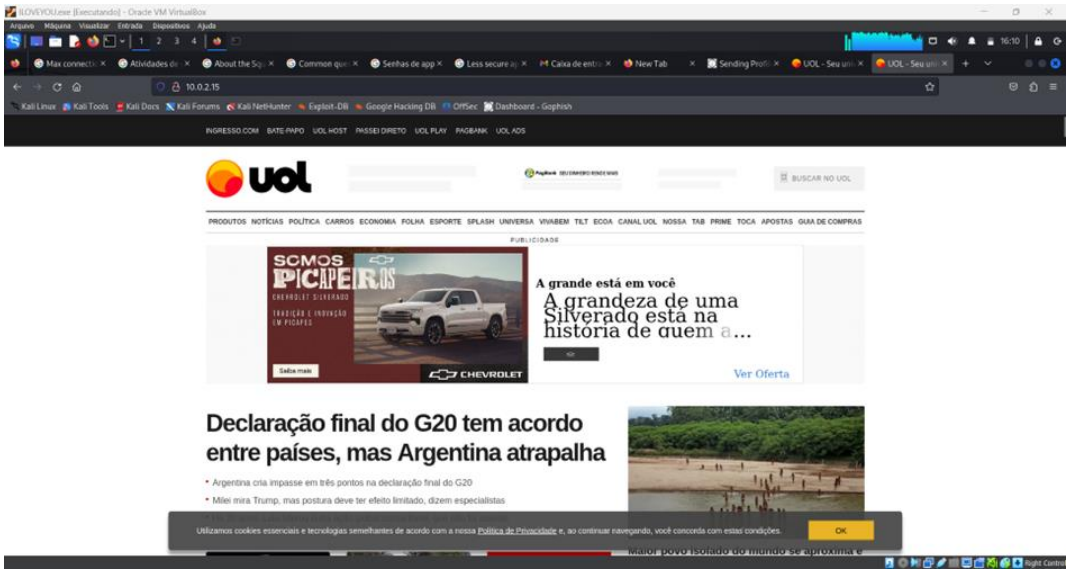

Em seguida, aparecerá um campo de colocar o IP. Caso não saiba seu IP, abra outro terminal e digite hostname -I. Depois insira nesse campo.



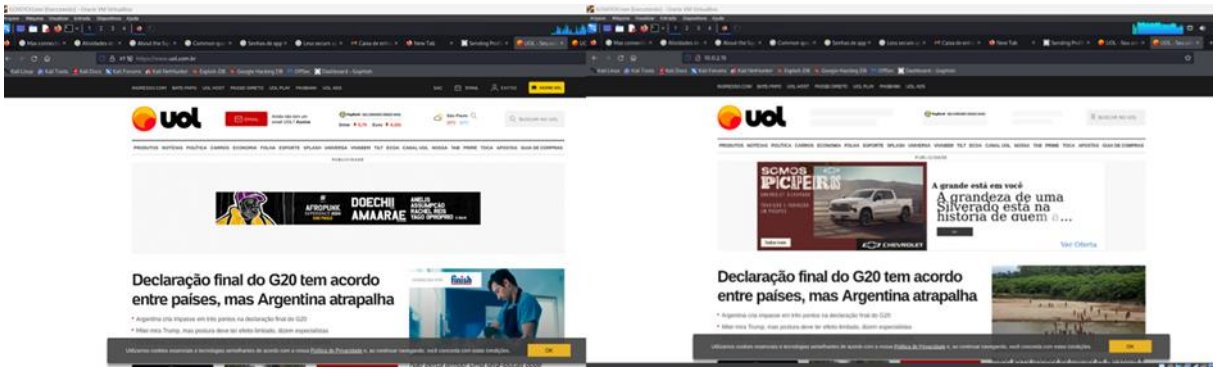

Depois, coloque o site que deseja clonar.




Minimiza o terminal e vá no navegador, pesquisando por *IP* na barra onde coloca o site. Esse é o resultado:



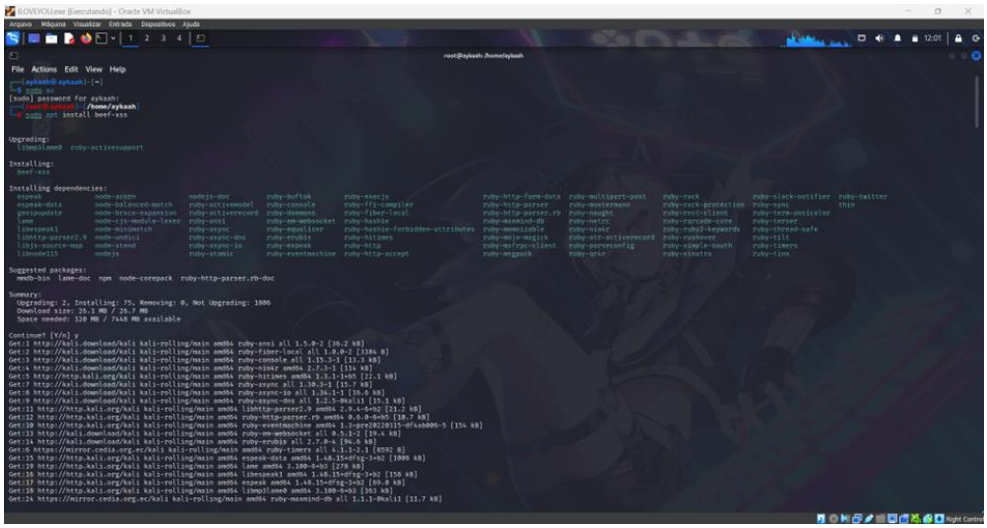

Comparação entre site original e site clonado:



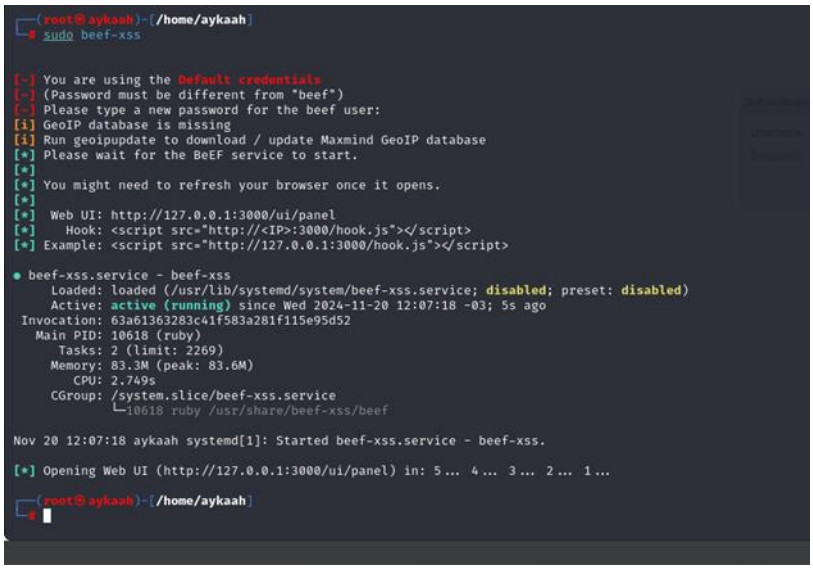

Embora o resultado gerado seja parecido, ainda é possível notar algumas pequenas diferenças sobre o site original. Além do link, que é diferente, no site original, a barra superior da *UOL* no site original aparece o preço do dólar e euro no momento e o clima em São Paulo, bem como uma aba para criar sua conta na *UOL*. No site clone, esses itens não foram renderizados, mesmo ficando quase idêntico ao original.

**BEEF**

Para começar, vamos instalar. Digite *sudo apt install beef-xss:*



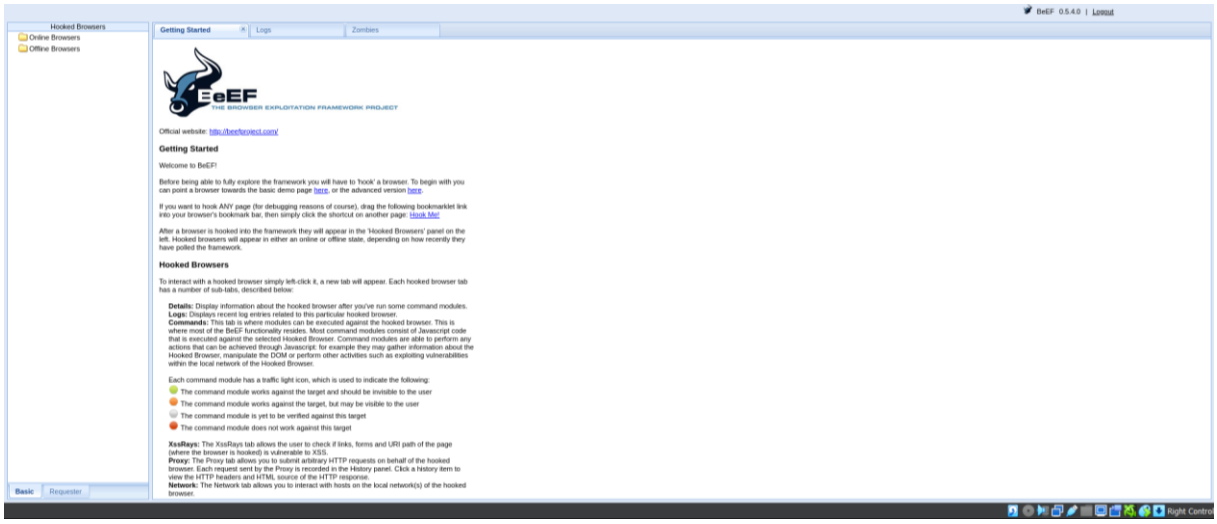
Para executar o programa, digite *sudo beef-xss*. Ao executar pela primeira vez, terá que alterar a senha padrão do usuário *Beef* para uma de sua preferência.




Depois de criar a senha, ele irá carregar e abrirá *WebUI* e o *script Hook* para *‘hook.js’*, para inserir em sites.


*BeEF* abrirá em uma página da *Web*, entre com o usuário ‘*beef’* e a senha que você configurou anteriormente.


Essa é a interface do *BeEF*:




Como cada aba funciona:

*Getting Started*: Orientações de como usar o *BeEF*, de forma geral.

*Logs*: O histórico de atividades do *BeEF*, incluindo interações com as páginas do navegador, comandos, respostas e erros do sistema.

*Zombies*: Terá navegadores que o *BeEF* controla, sendo listados, permitindo que interaja com eles.

*Hooked Browsers*: Lista de navegadores, que estão conectados atualmente no *BeEF*, contendo endereço *IP*, nome e Sistema Operacional.

*Requester*: Aba para enviar solicitação *HTTP* a partir do site logado no *BeEF*.

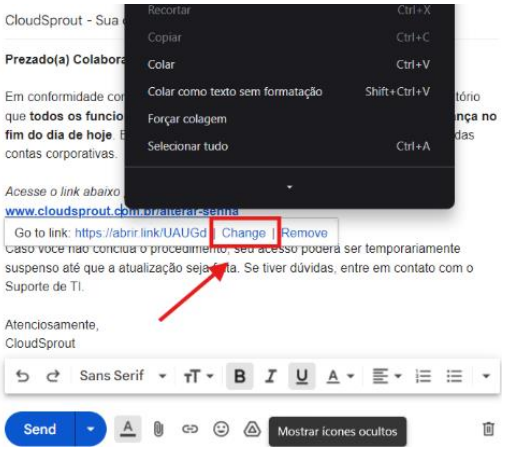
*Basic*: Para conferir mais informações sobre o navegador e interagir com o usuário (navegador) com comandos.

Na página inicial do *BeEF*, há dois links de demonstração, que podem ser testados e contém código malicioso (ou seja, *hook.js* dentro do *site*). Vamos testar do *'advanced version'*.

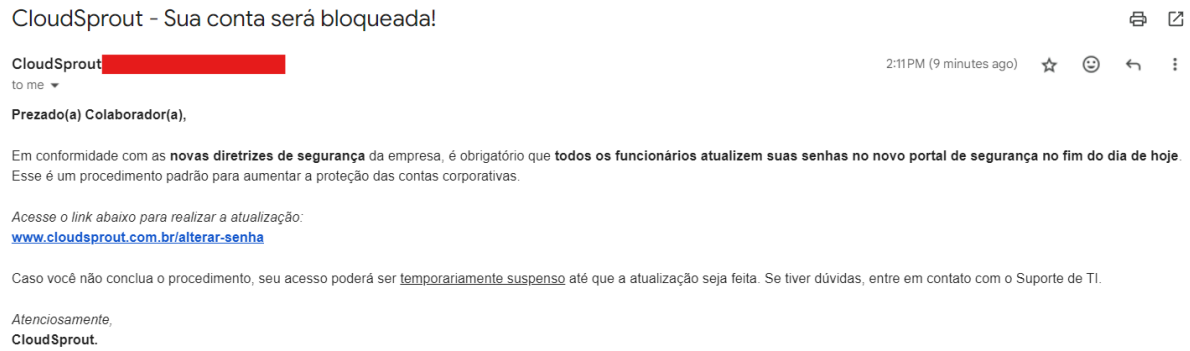
> Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page here, or the advanced version here.

Vamos copiar o *link*, ou seja, *http://127.0.0.1:3000/demos/butcher/index.html*. Recomendo que altere o *link* para o *IP* da sua máquina atacante.

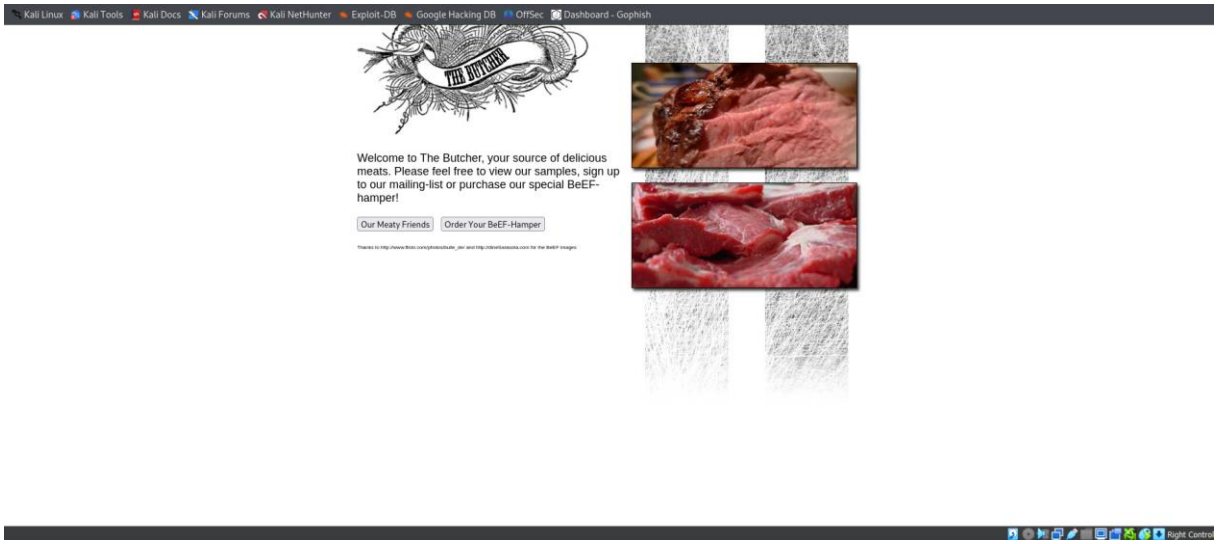
Vamos usar um encurtador de *URL* para enviar o *link* dentro de um *e-mail*, e usar depois o modificador do nome do *link* do próprio *Gmail*. Para mudar o nome do *link*, selecione, clique com o botão direito no *link* e clique em *Change*.



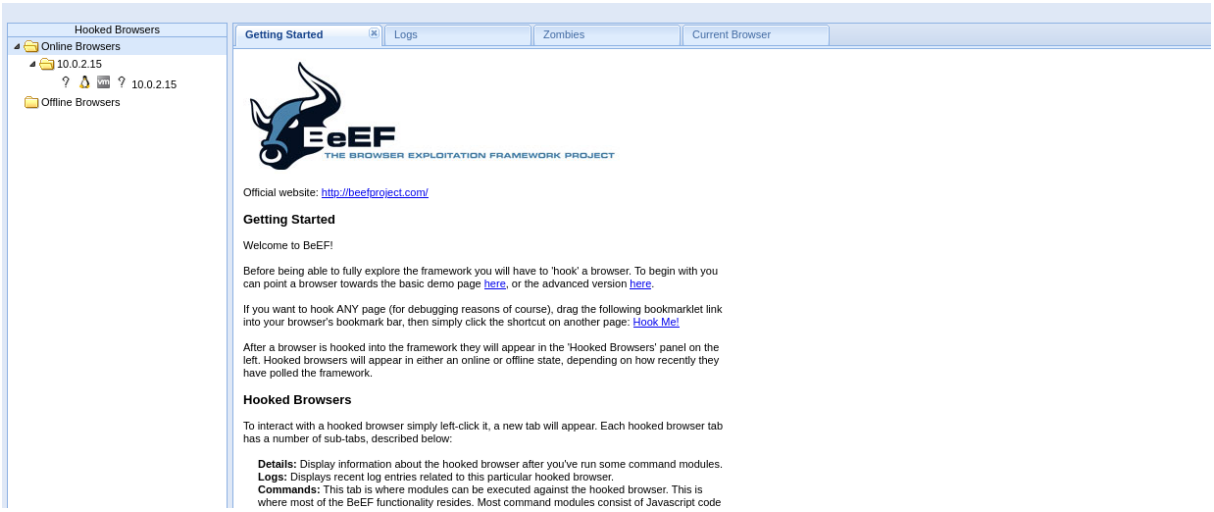

Enviamos uma simulação de *phishing* via *e-mail* para nós mesmos, e no caso, foi enviado para duas contas de *Gmail* que pertencem a mesma pessoa. Também pode ser testado via *GoPhish*, citado anteriormente.



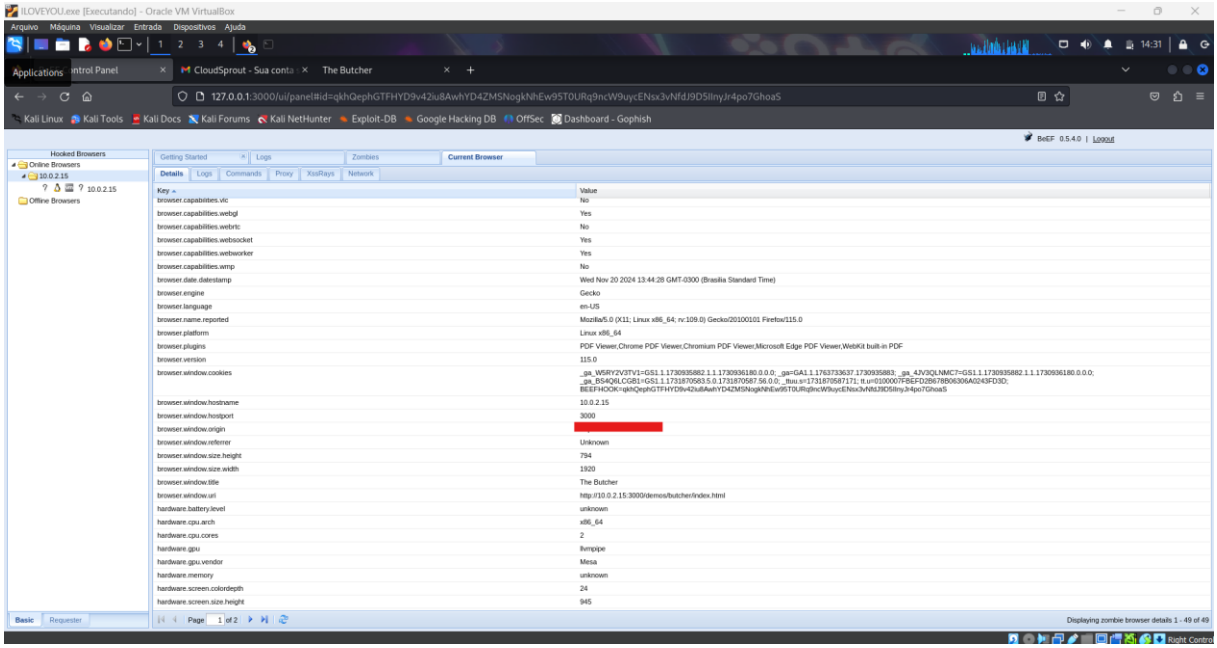

Quando o navegador (usuário) abrir, vai aparecer assim:



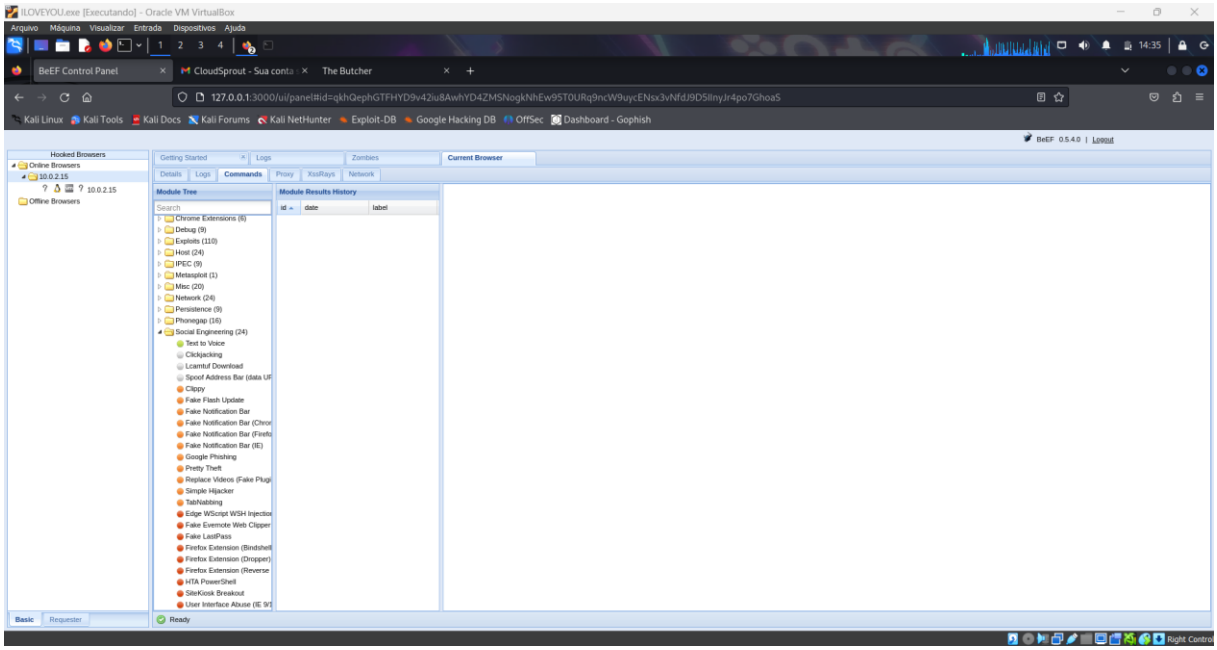

Um simples site de venda de carne. Confia...
Depois volte no *BeEF* e veja a surpresa:



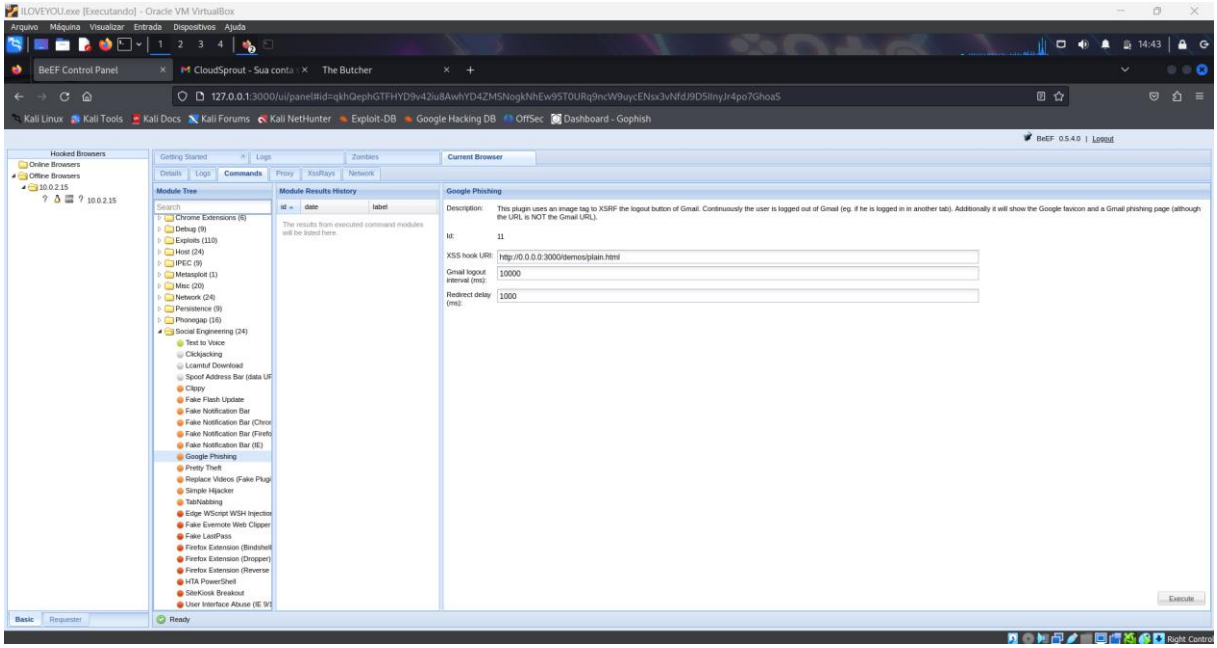

Olha o que aparece quando clica em "*Current Browser*":



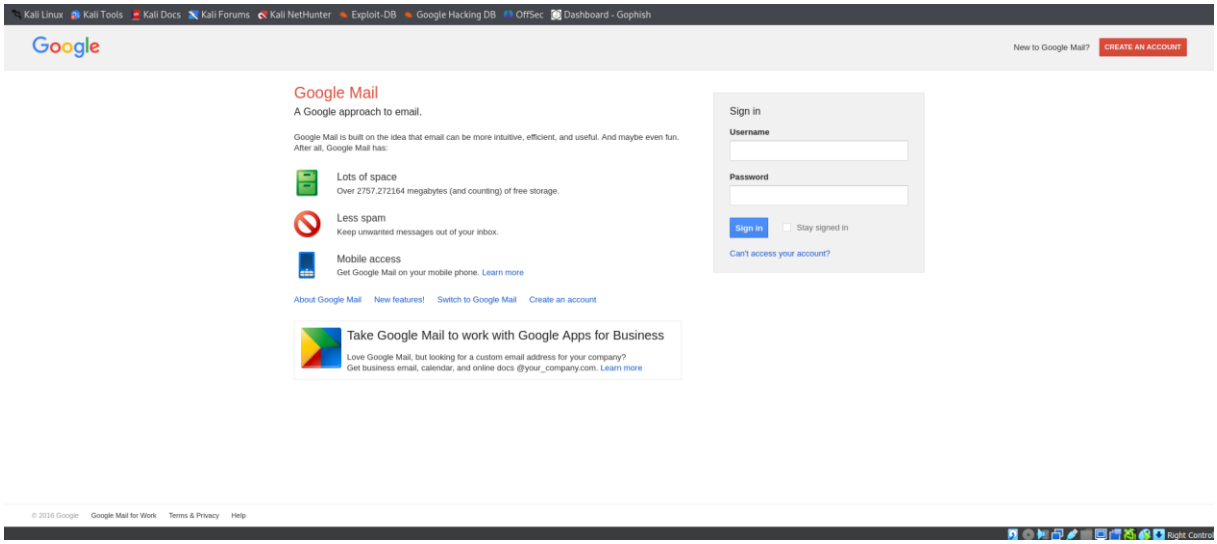
Em ‘*commands’*, podemos fazer comandos com nosso usuário. Mas por ora, iremos usar só a aba de Engenharia Social.



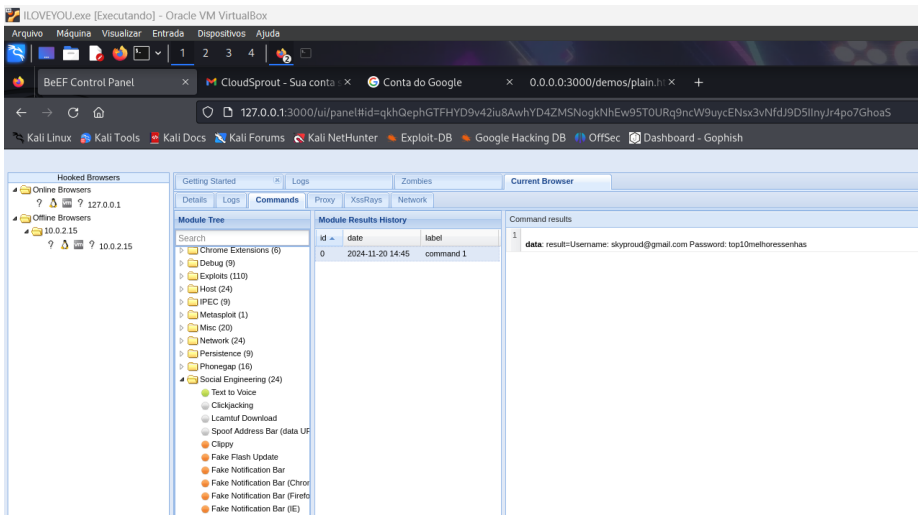
Vamos testar *Google Phishing* só de exemplo. Clique em *Google Phishing* e depois, vá em executar.



Olha, na página do navegante, foi solicitado conta do *Google*.



O que aparecerá no *BeEF* quando colocarem o *e-mail:*



**OSINT**

*Recon-ng:* Primeiro, abra o prompt de comando do seu *Linux*, e habilite *"sudo su"* para ativar o super-usuário. Se você usa *Kali Linux ou Parrot OS Security*, ele já vem pré-instalado, mas se tiver em outra distribuição, há algumas maneiras de instalar:

*Ubuntu*: Precisa de *git* e *pip* instalado. Siga os procedimentos.

*aykaah@aykaah:~/$ git clone https://github.com/lanmaster53/recon-ng.git*

*aykaah@aykaah:~/$ cd recon-ng*

*aykaah@aykaah:~/$ pip install -r REQUIREMENTS*

*aykaah@aykaah:~/recon-ng/$ ./recon-ng*

Usando *Docker*, siga esses procedimentos:

Instale *Docker Desktop*;

Veja se *~/.recon-ng* tem no *host*;

Clone o repositório *GitHub*

- *git clone https://github.com/lanmaster53/recon-ng.git*

Mude o diretório para *Recon-ng*;

- *cd recon-ng*

Construa a imagem do *Docker*;

*docker build --rm -t recon-ng .*

Execute *recon-ng*;

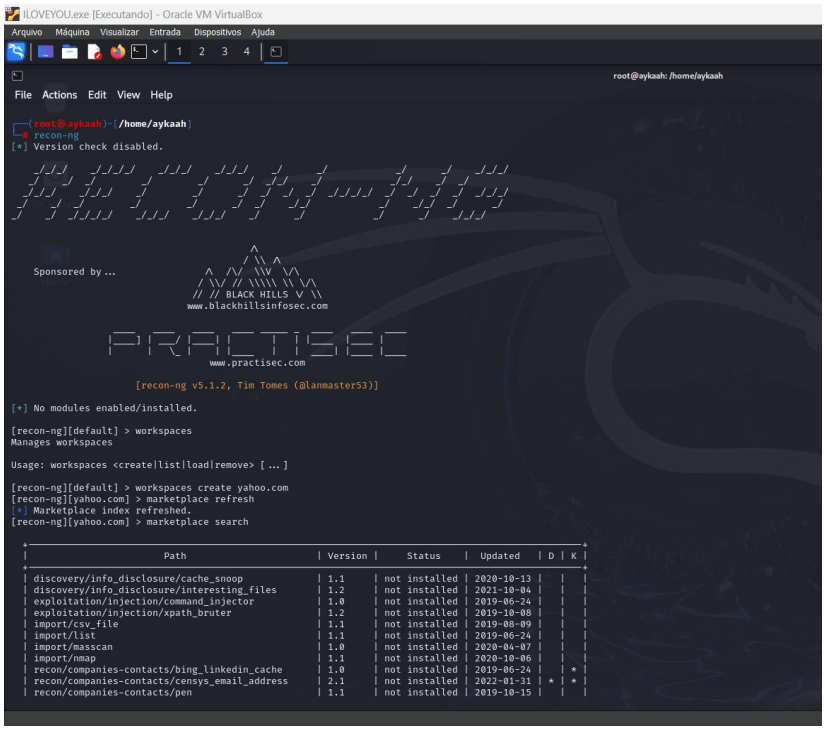
*docker run --rm -it -p 5000:5000 -v $(pwd):/recon-ng -v ~/.recon-ng:/root/.recon-ng --entrypoint "./recon-ng" recon-ng*

Ao iniciar Recon-web, *--entrypoint "./recon-web"* e *--host 0.0.0.0* deve ser anexado no final do comando.

Execute *API* com *docker-compose up -d --build*

Ao terminar de usar, digite *docker-compose down*

**Uso***:*



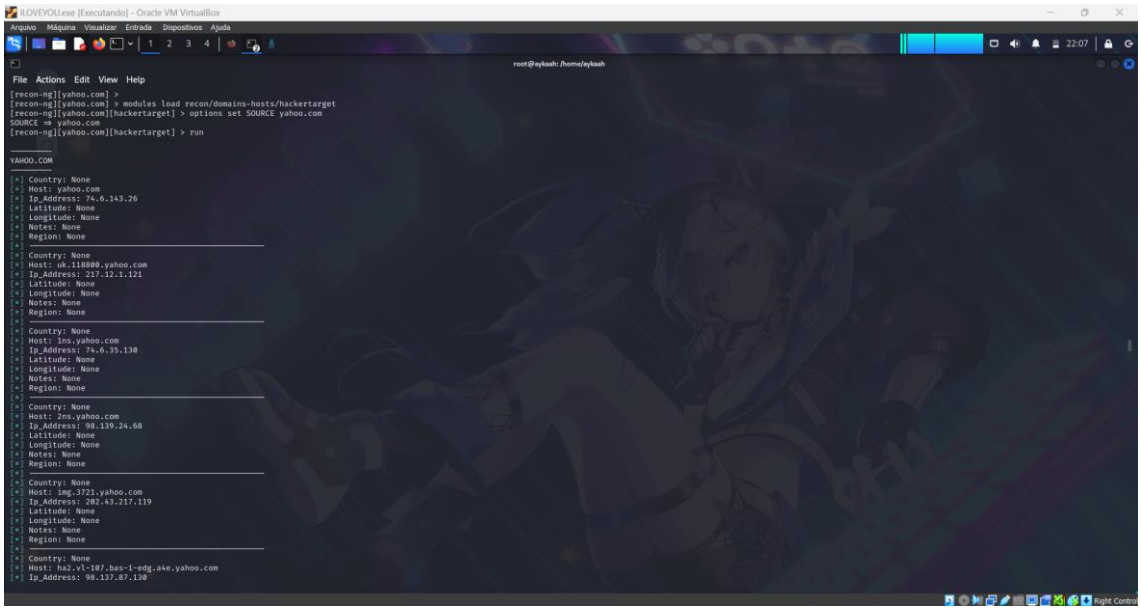

Para executar, digite *recon-ng*

Ao abrir, precisaremos criar uma *workspaces*. Digite *workspaces create nomequedesejarcolocar.*

Depois, precisamos atualizar os *marketplaces*, ou seja, um repositório de comandos que podem ser usados nessa ferramenta. Para atualizar a lista para a última versão, digite *marketplace refresh*. Depois, para pesquisar as ferramentas, pesquise *marketplace search*.

Um comando que recomendo para baixar vários *marketplaces* ao mesmo tempo é o *marketplace install all.*

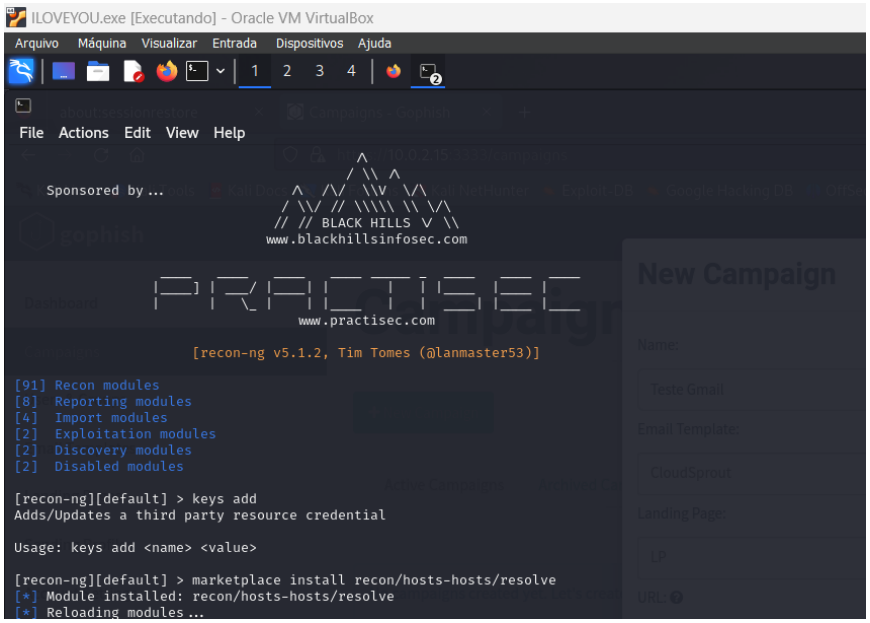
Uma das ferramentas que existe, que coleta *IP* é o *HackerTarget*. Digite *marketplace install recon/domains-hosts/hackertarget.*



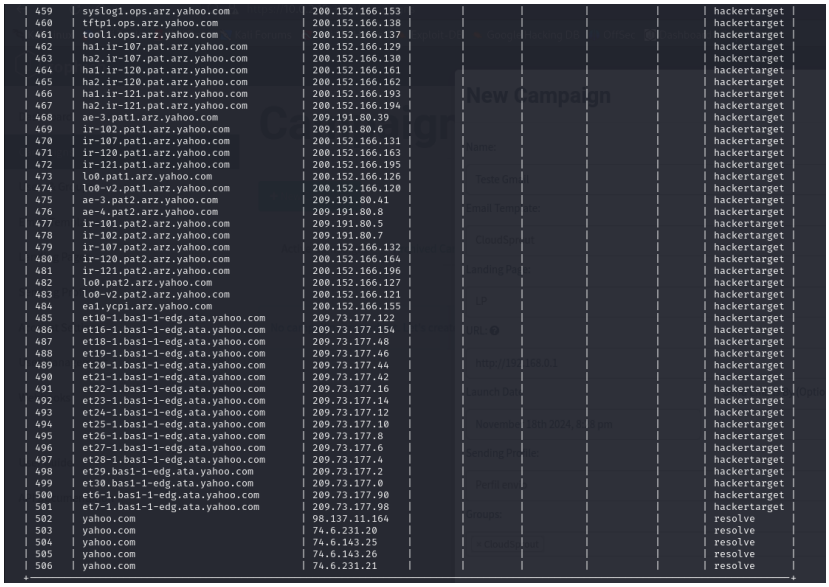

Para baixar o módulo, escreva *modules load recon/domains-hosts/hackertarget* e depois escreva *info*, conforme a *print*.

Para extrair *IPs* de um *site*, escreve-se *options set SOURCE sitequedesejar.com* (no caso da *print*, foi *yahoo.com*).

Outros comandos por *IP* podem ser encontrados usando *recon/hosts-hosts/resolve*, assim como o *bing_ip, ipinfodb, ipstack e shodan_ip* também podem ser usados para esse fim. No caso, vamos usar recon/hosts-hosts/resolve. Digite *marketplace install recon/hosts-hosts/resolve*, depois rode *modules load recon/hosts-hosts/resolve*, e depois *info*. Depois, coloque *options set SOURCE sitequedesejar.com* (aqui foi *yahoo.com*). Em seguida, *run*.

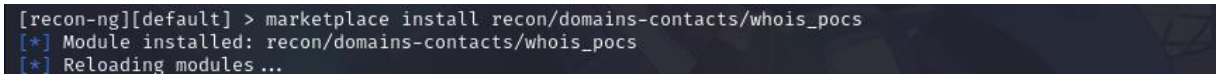


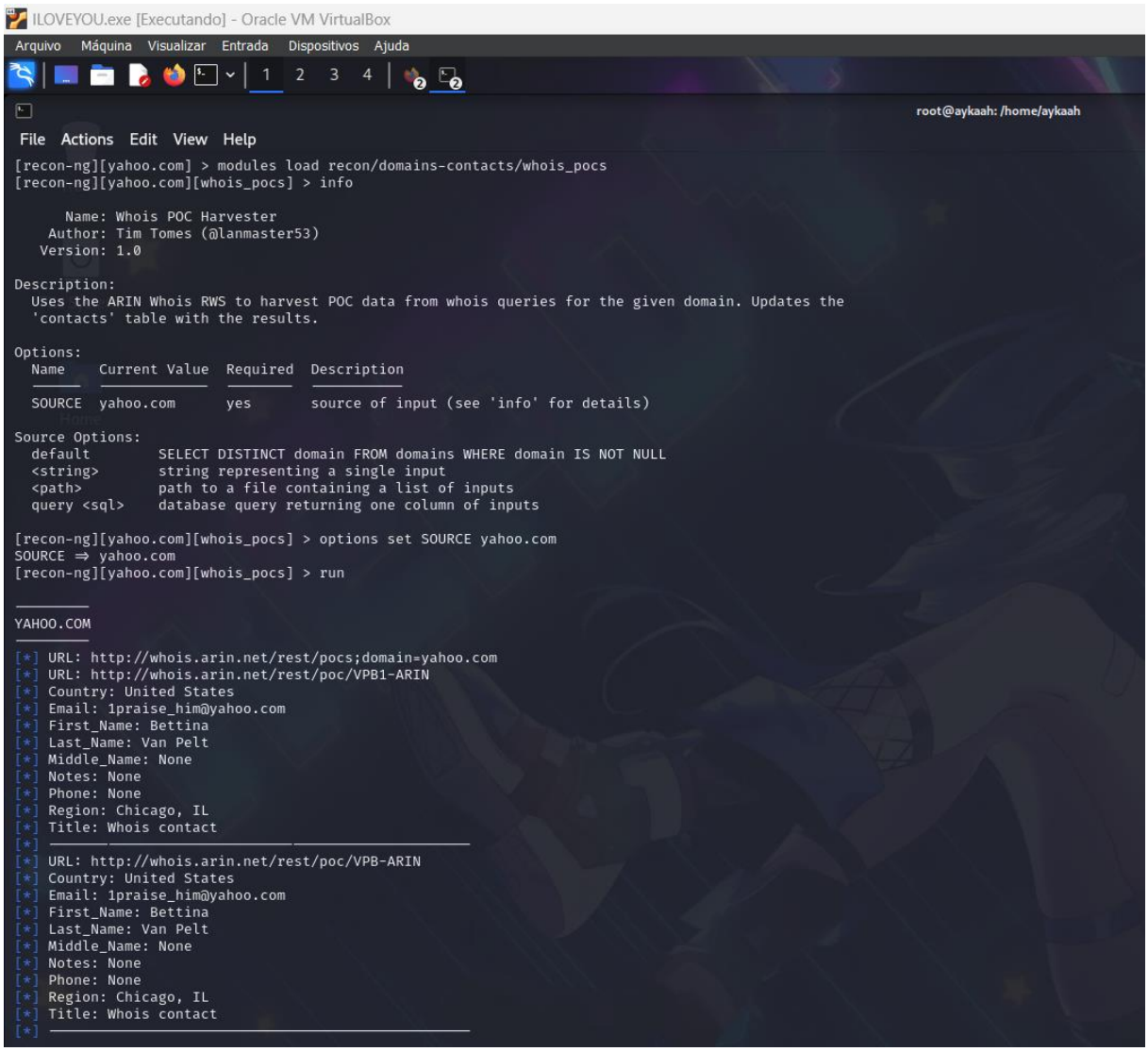

Para ver quantos *hosts* já capturou até agora, digite *show hosts*.



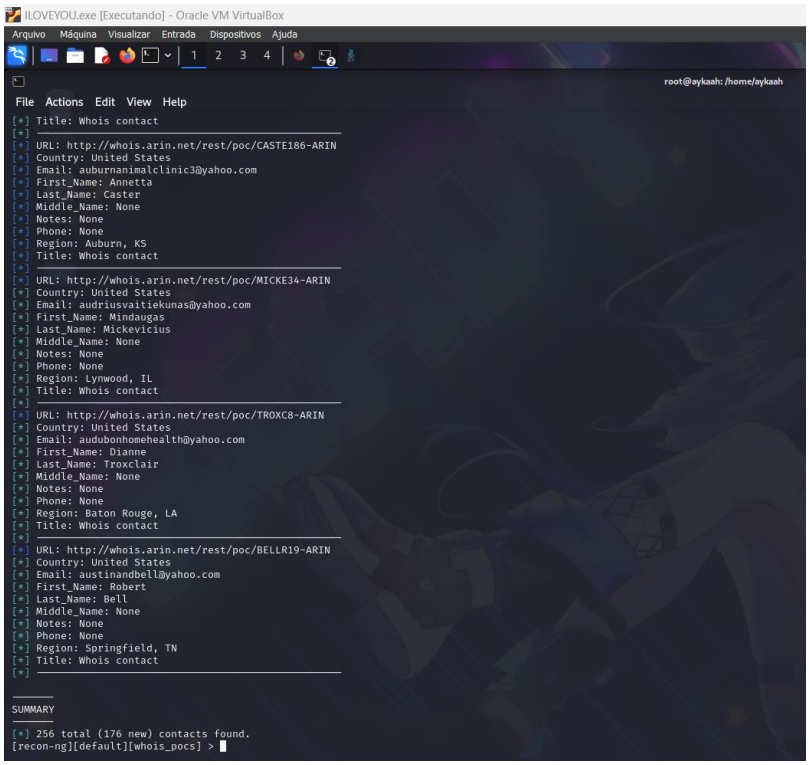
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 459 | syslog1.ops.arz.yahoo.com | 200.152.166.153 | | | | | hackertarget |
| 460 | tftp1.ops.arz.yahoo.com | 200.152.166.138 | | | | | hackertarget |
| 461 | tool1.ops.arz.yahoo.com | 200.152.166.137 | | | | | hackertarget |
| 462 | ha1.ir-107.pat.arz.yahoo.com | 200.152.166.129 | | | | | hackertarget |
| 463 | ha2.ir-107.pat.arz.yahoo.com | 200.152.166.130 | | | | | hackertarget |
| 464 | ha1.ir-120.pat.arz.yahoo.com | 200.152.166.161 | | | | | hackertarget |
| 465 | ha2.ir-120.pat.arz.yahoo.com | 200.152.166.162 | | | | | hackertarget |
| 466 | ha1.ir-121.pat.arz.yahoo.com | 200.152.166.193 | | | | | hackertarget |
| 467 | ha2.ir-121.pat.arz.yahoo.com | 200.152.166.194 | | | | | hackertarget |
| 468 | ae-3.pat1.arz.yahoo.com | 209.191.80.39 | | | | | hackertarget |
| 469 | ir-102.pat1.arz.yahoo.com | 209.191.80.6 | | | | | hackertarget |
| 470 | ir-107.pat1.arz.yahoo.com | 200.152.166.131 | | | | | hackertarget |
| 471 | ir-120.pat1.arz.yahoo.com | 200.152.166.163 | | | | | hackertarget |
| 472 | ir-121.pat1.arz.yahoo.com | 200.152.166.195 | | | | | hackertarget |
| 473 | lo0.pat1.arz.yahoo.com | 200.152.166.126 | | | | | hackertarget |
| 474 | lo0-v2.pat1.arz.yahoo.com | 200.152.166.120 | | | | | hackertarget |
| 475 | ae-3.pat2.arz.yahoo.com | 209.191.80.41 | | | | | hackertarget |
| 476 | ae-4.pat2.arz.yahoo.com | 209.191.80.8 | | | | | hackertarget |
| 477 | ir-101.pat2.arz.yahoo.com | 209.191.80.5 | | | | | hackertarget |
| 478 | ir-102.pat2.arz.yahoo.com | 209.191.80.7 | | | | | hackertarget |
| 479 | ir-107.pat2.arz.yahoo.com | 200.152.166.132 | | | | | hackertarget |
| 480 | ir-120.pat2.arz.yahoo.com | 200.152.166.164 | | | | | hackertarget |
| 481 | ir-121.pat2.arz.yahoo.com | 200.152.166.196 | | | | | hackertarget |
| 482 | lo0.pat2.arz.yahoo.com | 200.152.166.127 | | | | | hackertarget |
| 483 | lo0-v2.pat2.arz.yahoo.com | 200.152.166.121 | | | | | hackertarget |
| 484 | ea1.ycpi.arz.yahoo.com | 200.152.166.155 | | | | | hackertarget |
| 485 | et10-1.bas1-1-edg.ata.yahoo.com | 209.73.177.122 | | | | | hackertarget |
| 486 | et16-1.bas1-1-edg.ata.yahoo.com | 209.73.177.154 | | | | | hackertarget |
| 487 | et18-1.bas1-1-edg.ata.yahoo.com | 209.73.177.48 | | | | | hackertarget |
| 488 | et19-1.bas1-1-edg.ata.yahoo.com | 209.73.177.46 | | | | | hackertarget |
| 489 | et20-1.bas1-1-edg.ata.yahoo.com | 209.73.177.44 | | | | | hackertarget |
| 490 | et21-1.bas1-1-edg.ata.yahoo.com | 209.73.177.42 | | | | | hackertarget |
| 491 | et22-1.bas1-1-edg.ata.yahoo.com | 209.73.177.16 | | | | | hackertarget |
| 492 | et23-1.bas1-1-edg.ata.yahoo.com | 209.73.177.14 | | | | | hackertarget |
| 493 | et24-1.bas1-1-edg.ata.yahoo.com | 209.73.177.12 | | | | | hackertarget |
| 494 | et25-1.bas1-1-edg.ata.yahoo.com | 209.73.177.10 | | | | | hackertarget |
| 495 | et26-1.bas1-1-edg.ata.yahoo.com | 209.73.177.8 | | | | | hackertarget |
| 496 | et27-1.bas1-1-edg.ata.yahoo.com | 209.73.177.6 | | | | | hackertarget |
| 497 | et28-1.bas1-1-edg.ata.yahoo.com | 209.73.177.4 | | | | | hackertarget |
| 498 | et29.bas1-1-edg.ata.yahoo.com | 209.73.177.2 | | | | | hackertarget |
| 499 | et30.bas1-1-edg.ata.yahoo.com | 209.73.177.0 | | | | | hackertarget |
| 500 | et6-1.bas1-1-edg.ata.yahoo.com | 209.73.177.90 | | | | | hackertarget |
| 501 | et7-1.bas1-1-edg.ata.yahoo.com | 209.73.177.98 | | | | | hackertarget |
| 502 | yahoo.com | 98.137.11.164 | | | | | resolve |
| 503 | yahoo.com | 74.6.231.20 | | | | | resolve |
| 504 | yahoo.com | 74.6.143.25 | | | | | resolve |
| 505 | yahoo.com | 74.6.143.26 | | | | | resolve |
| 506 | yahoo.com | 74.6.231.21 | | | | | resolve |

Agora, iremos rodar o *recon/domains-contacts/whois_pocs*, para coletar *e-mails* disponíveis publicamente. Siga esses procedimentos: *marketplace install recon/domains-contacts/whois_pocs*, depois volte para *o workspaces* com *workspaces load yahoo.com*, digite *modules load recon/domains-contacts/whois_pocs*, vá em *info*, segue com *options set SOURCE yahoo.com*, e *run*






Nesse caso, foi encontrado 176 contatos relacionados com *yahoo.com* apenas com essa ferramenta, tendo um total de 256 até agora.




Escrevendo *show hosts*, dá para ver todos os endereços *IP* coletados, e escrevendo *show contacts*, dá para ver todos os contatos obtidos pelo *whois*.

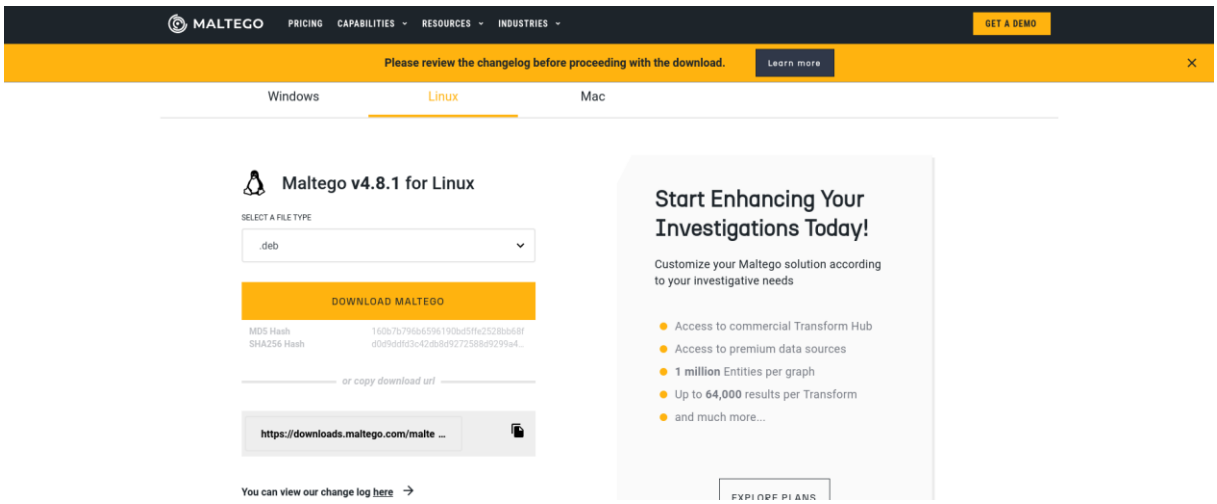
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 453 | dns-hv1.ops.arz.yahoo.com | 200.152.166.180 | | | | | | hackertarget |
| 454 | dns-hv2.ops.arz.yahoo.com | 200.152.166.181 | | | | | | hackertarget |
| 455 | mrtg1.ops.arz.yahoo.com | 200.152.166.151 | | | | | | hackertarget |
| 456 | netflow-01.ops.arz.yahoo.com | 200.152.166.154 | | | | | | hackertarget |
| 457 | netlog1.ops.arz.yahoo.com | 200.152.166.152 | | | | | | hackertarget |
| 458 | ipalias.netlog1.ops.arz.yahoo.com | 200.152.166.149 | | | | | | hackertarget |
| 459 | syslog1.ops.arz.yahoo.com | 200.152.166.153 | | | | | | hackertarget |
| 460 | tftp1.ops.arz.yahoo.com | 200.152.166.138 | | | | | | hackertarget |
| 461 | tool1.ops.arz.yahoo.com | 200.152.166.137 | | | | | | hackertarget |
| 462 | ha1.ir-107.pat.arz.yahoo.com | 200.152.166.129 | | | | | | hackertarget |
| 463 | ha2.ir-107.pat.arz.yahoo.com | 200.152.166.130 | | | | | | hackertarget |
| 464 | ha1.ir-120.pat.arz.yahoo.com | 200.152.166.161 | | | | | | hackertarget |
| 465 | ha2.ir-120.pat.arz.yahoo.com | 200.152.166.162 | | | | | | hackertarget |
| 466 | ha1.ir-121.pat.arz.yahoo.com | 200.152.166.193 | | | | | | hackertarget |
| 467 | ha2.ir-121.pat.arz.yahoo.com | 200.152.166.194 | | | | | | hackertarget |
| 468 | ae-3.pat1.arz.yahoo.com | 209.191.80.39 | | | | | | hackertarget |
| 469 | ir-102.pat1.arz.yahoo.com | 209.191.80.6 | | | | | | hackertarget |
| 470 | ir-107.pat1.arz.yahoo.com | 200.152.166.131 | | | | | | hackertarget |
| 471 | ir-120.pat1.arz.yahoo.com | 200.152.166.163 | | | | | | hackertarget |
| 472 | ir-121.pat1.arz.yahoo.com | 200.152.166.195 | | | | | | hackertarget |
| 473 | lo0.pat1.arz.yahoo.com | 200.152.166.126 | | | | | | hackertarget |
| 474 | lo0-v2.pat1.arz.yahoo.com | 200.152.166.120 | | | | | | hackertarget |
| 475 | ae-3.pat2.arz.yahoo.com | 209.191.80.41 | | | | | | hackertarget |
| 476 | ae-4.pat2.arz.yahoo.com | 209.191.80.8 | | | | | | hackertarget |
| 477 | ir-101.pat2.arz.yahoo.com | 209.191.80.5 | | | | | | hackertarget |
| 478 | ir-102.pat2.arz.yahoo.com | 209.191.80.7 | | | | | | hackertarget |
| 479 | ir-107.pat2.arz.yahoo.com | 200.152.166.132 | | | | | | hackertarget |
| 480 | ir-120.pat2.arz.yahoo.com | 200.152.166.164 | | | | | | hackertarget |
| 481 | ir-121.pat2.arz.yahoo.com | 200.152.166.196 | | | | | | hackertarget |
| 482 | lo0.pat2.arz.yahoo.com | 200.152.166.127 | | | | | | hackertarget |
| 483 | lo0-v2.pat2.arz.yahoo.com | 200.152.166.121 | | | | | | hackertarget |
| 484 | ea1.ycpi.arz.yahoo.com | 200.152.166.155 | | | | | | hackertarget |
| 485 | et10-1.bas1-1-edg.ata.yahoo.com | 209.73.177.122 | | | | | | hackertarget |
| 486 | et16-1.bas1-1-edg.ata.yahoo.com | 209.73.177.154 | | | | | | hackertarget |
| 487 | et18-1.bas1-1-edg.ata.yahoo.com | 209.73.177.48 | | | | | | hackertarget |
| 488 | et19-1.bas1-1-edg.ata.yahoo.com | 209.73.177.46 | | | | | | hackertarget |
| 489 | et20-1.bas1-1-edg.ata.yahoo.com | 209.73.177.44 | | | | | | hackertarget |
| 490 | et21-1.bas1-1-edg.ata.yahoo.com | 209.73.177.42 | | | | | | hackertarget |
| 491 | et22-1.bas1-1-edg.ata.yahoo.com | 209.73.177.16 | | | | | | hackertarget |
| 492 | et23-1.bas1-1-edg.ata.yahoo.com | 209.73.177.14 | | | | | | hackertarget |
| 493 | et24-1.bas1-1-edg.ata.yahoo.com | 209.73.177.12 | | | | | | hackertarget |
| 494 | et25-1.bas1-1-edg.ata.yahoo.com | 209.73.177.10 | | | | | | hackertarget |
| 495 | et26-1.bas1-1-edg.ata.yahoo.com | 209.73.177.8 | | | | | | hackertarget |
| 496 | et27-1.bas1-1-edg.ata.yahoo.com | 209.73.177.6 | | | | | | hackertarget |
| 497 | et28-1.bas1-1-edg.ata.yahoo.com | 209.73.177.4 | | | | | | hackertarget |
| 498 | et29.bas1-1-edg.ata.yahoo.com | 209.73.177.2 | | | | | | hackertarget |
| 499 | et30.bas1-1-edg.ata.yahoo.com | 209.73.177.0 | | | | | | hackertarget |
| 500 | et6-1.bas1-1-edg.ata.yahoo.com | 209.73.177.90 | | | | | | hackertarget |
| 501 | et7-1.bas1-1-edg.ata.yahoo.com | 209.73.177.98 | | | | | | hackertarget |
| 502 | yahoo.com | 74.6.231.20 | | | | | | resolve |
| 503 | yahoo.com | 74.6.143.26 | | | | | | resolve |
| 504 | yahoo.com | 74.6.143.25 | | | | | | resolve |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 123 | Angel | | Domenech | angeldmail@yahoo.com | Whois contact | Cg, FL | United States | | whois_pocs |
| 124 | Angela | | Krcmar | angie_krcmar@yahoo.com | Whois contact | Barrington, IL | United States | | whois_pocs |
| 125 | simpson | | angie | angiesimpson@yahoo.com | Whois contact | Gilsvl, GA | United States | | whois_pocs |
| 126 | Angela | | Snyder | ang.snyder@yahoo.com | Whois contact | Bastrop, TX | United States | | whois_pocs |
| 127 | Tracy | | Sprunger | animalarkofarcadia@yahoo.com | Whois contact | Arcadia, FL | United States | | whois_pocs |
| 128 | Anis | | Khwahja | anisk@yahoo.com | Whois contact | Howard Beach, NY | United States | | whois_pocs |
| 129 | Ankur | | Prashar | ankur.prashar@yahoo.com | Whois contact | Baker City, OR | United States | | whois_pocs |
| 130 | Ann | | L'altrella | annlaltrella@yahoo.com | Whois contact | Huntington, CT | United States | | whois_pocs |
| 131 | steve | | anstey | anst2u@yahoo.com | Whois contact | Champaign, IL | United States | | whois_pocs |
| 132 | ANTHONY | | CALDERON | antcal310@yahoo.com | Whois contact | Ant, CA | United States | | whois_pocs |
| 133 | Anthea | | Harbin | anthea.harbin@yahoo.com | Whois contact | Carthage, MO | United States | | whois_pocs |
| 134 | Yael | | Nimon | anthonyho1@yahoo.com | Whois contact | Boston, MA | United States | | whois_pocs |
| 135 | Glenford | | Lettman | anthonylettman@yahoo.com | Whois contact | Kingston, ST. ANDREW | Jamaica | | whois_pocs |
| 136 | Anthony | | Warnock | anthonywarnock@yahoo.com | Whois contact | Orl, FL | United States | | whois_pocs |
| 137 | ADAM | | PALAZZARI | apalazza@yahoo.com | Whois contact | Lafayette, CO | United States | | whois_pocs |
| 138 | Maisy | | Okonkwo | apexpa1800@yahoo.com | Whois contact | Ocala, FL | United States | | whois_pocs |
| 139 | DAVID | | WILKERSON | aplospharm96@yahoo.com | Whois contact | Bonifay, FL | United States | | whois_pocs |
| 140 | David | | Wilkerson | aplospharm96@yahoo.com | Whois contact | Bonifay, FL | United States | | whois_pocs |
| 141 | APRIL | | MARTIN | april_georgebrothers@yahoo.com | Whois contact | Odessa, TX | United States | | whois_pocs |
| 142 | Aras | | Mardosa | Aras.Mardosa@yahoo.com | Whois contact | Laguna Woods, CA | United States | | whois_pocs |
| 143 | CHRIS | | ARBAUGH | arbaugh100@yahoo.com | Whois contact | Colorado Springs, CO | United States | | whois_pocs |
| 144 | Gary | | Nevin | argobuilding@yahoo.com | Whois contact | Birmingham, AL | United States | | whois_pocs |
| 145 | ARJANA | | ROSIC | arjana29@yahoo.com | Whois contact | Waterloo, IA | United States | | whois_pocs |
| 146 | Erik | | Sowirka | arksow@yahoo.com | Whois contact | Gilbert, AZ | United States | | whois_pocs |
| 147 | Arlene | | Kitson | arlenekitson@yahoo.com | Whois contact | Warsaw, IN | United States | | whois_pocs |
| 148 | ARLENE | | KITSON | arlenekitson@yahoo.com | Whois contact | Syracuse, IN | United States | | whois_pocs |
| 149 | Robert | | Brink | arlingtoni@yahoo.com | Whois contact | Mission Viejo, CA | United States | | whois_pocs |
| 150 | Arman | | Khalili | arman4711@yahoo.com | Whois contact | Montrose, CA | United States | | whois_pocs |
| 151 | Domingo | | Saez | arnaldo_mail@yahoo.com | Whois contact | Corozal, PR | Puerto Rico | | whois_pocs |
| 152 | ANTONIO | | ROBLES | arobles926@yahoo.com | Whois contact | Sm, FL | United States | | whois_pocs |
| 153 | DENNIS | | ARONHALT | aronhalt1977@yahoo.com | Whois contact | Bonifay, FL | United States | | whois_pocs |
| 154 | Arturo | | Godoy | art_motoportusa@yahoo.com | Whois contact | Mia, FL | United States | | whois_pocs |
| 155 | ARUN | | PATEL | arunpatel42@yahoo.com | Whois contact | Albuquerque, NM | United States | | whois_pocs |
| 156 | ALLAN | | MONK | asap_ut@yahoo.com | Whois contact | St George, UT | United States | | whois_pocs |
| 157 | RAY | | SHOUTEN | asc_ray@yahoo.com | Whois contact | Phoenix, AZ | United States | | whois_pocs |
| 158 | Amina | | Sehwail | asehwail1114@yahoo.com | Whois contact | Glenvw, IL | United States | | whois_pocs |
| 159 | | | ABUSE MAILBOX | asfandkhawar2017@yahoo.com | Whois contact | Lahore | Pakistan | | whois_pocs |
| 160 | Asfand | | Khawar | asfandkhawar2017@yahoo.com | Whois contact | Lahore | Pakistan | | whois_pocs |
| 161 | Tracy | | Ashe | ashe.tracy@yahoo.com | Whois contact | Pndrgras, GA | United States | | whois_pocs |
| 162 | ASHISH | | PATEL | ashish_patel501@yahoo.com | Whois contact | Tpsa, GA | United States | | whois_pocs |
| 163 | Ashley | | Dunckel | ashleyd_princeton@yahoo.com | Whois contact | Johns Creek, GA | United States | | whois_pocs |
| 164 | Ashely | | Hong | ashley.hong@yahoo.com | Whois contact | Ver, CA | United States | | whois_pocs |
| 165 | Ashley | | Bell | ashley_nichole_bell@yahoo.com | Whois contact | Woodward, OK | United States | | whois_pocs |
| 166 | Sam | | Quattrochi | asonofitaly@yahoo.com | Whois contact | Golden, CO | United States | | whois_pocs |
| 167 | Meg | | Emeruwa | aspenmedical_group@yahoo.com | Whois contact | Riverside, CA | United States | | whois_pocs |
| 168 | Assaf | | Levy | assi_lev@yahoo.com | Whois contact | Boston, MA | United States | | whois_pocs |
| 169 | Loren | | Pochirowski | astroncorporation@yahoo.com | Whois contact | Irv, CA | United States | | whois_pocs |
| 170 | Jim | | Payne | atcoautosupply@yahoo.com | Whois contact | Atchison, KS | United States | | whois_pocs |
| 171 | Andre | | Landry | atsi6754@yahoo.com | Whois contact | Pierre Part, LA | United States | | whois_pocs |
| 172 | Girum | | Hailemariam | hailegr@yahoo.com | Whois contact | Carpentersville, IL | United States | | whois_pocs |
| 173 | Annetta | | Caster | auburnanimalclinic3@yahoo.com | Whois contact | Auburn, KS | United States | | whois_pocs |
| 174 | Mindaugas | | Mickevicius | audriusvaitiekunas@yahoo.com | Whois contact | Lynwood, IL | United States | | whois_pocs |

**MALTEGO**

Se você usa *Kali Linux ou Parrot OS Security*, ele já vem instalado. Mas se quiser instalar em outra distribuição *Linux*, como *Ubuntu, Debian, Fedora* etc., siga esses procedimentos.

Vá em *https://www.maltego.com/downloads/;*




Na aba *Linux*, escolha se quer *.deb, .zip ou .rpm*;

Se foi *.deb*, vá no terminal, e digite *cd Downloads* e depois *cd Maltego* (Caso você tenha instalado nessa pasta) e em seguida *dpkg –i <maltegofile>.deb*

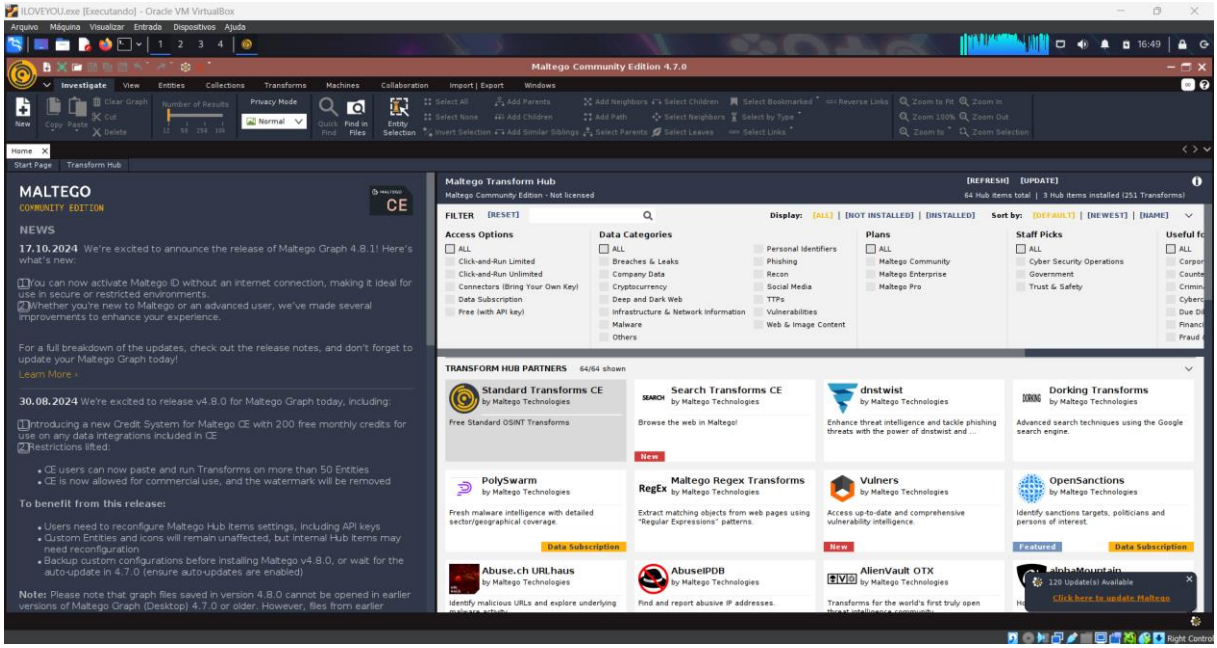
Se foi *.rpm*, no terminal, digite *cd Downloads* e depois *cd Maltego* (Supondo que você instalou nessa pasta). Em seguida, *rpm –i <maltegofile>.rpm*

Se foi *.zip*, extraia o arquivo e rode *Maltego* no diretório *bin*.

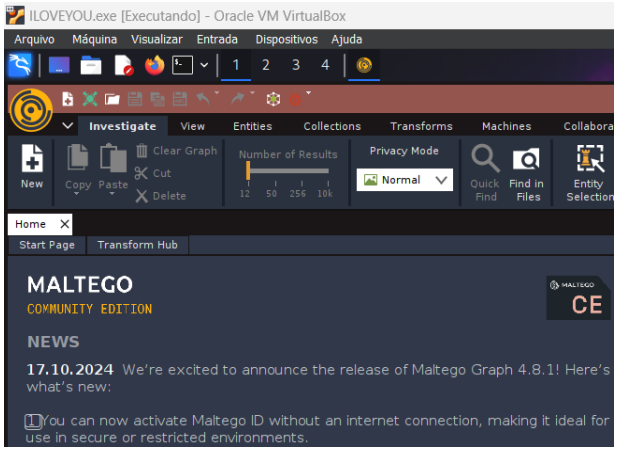
Também é possível instalar no *Windows e Mac*.

Ao instalar, irá pedir para que você se registre com *Maltego ID*. Crie sua conta e siga os procedimentos fornecidos.

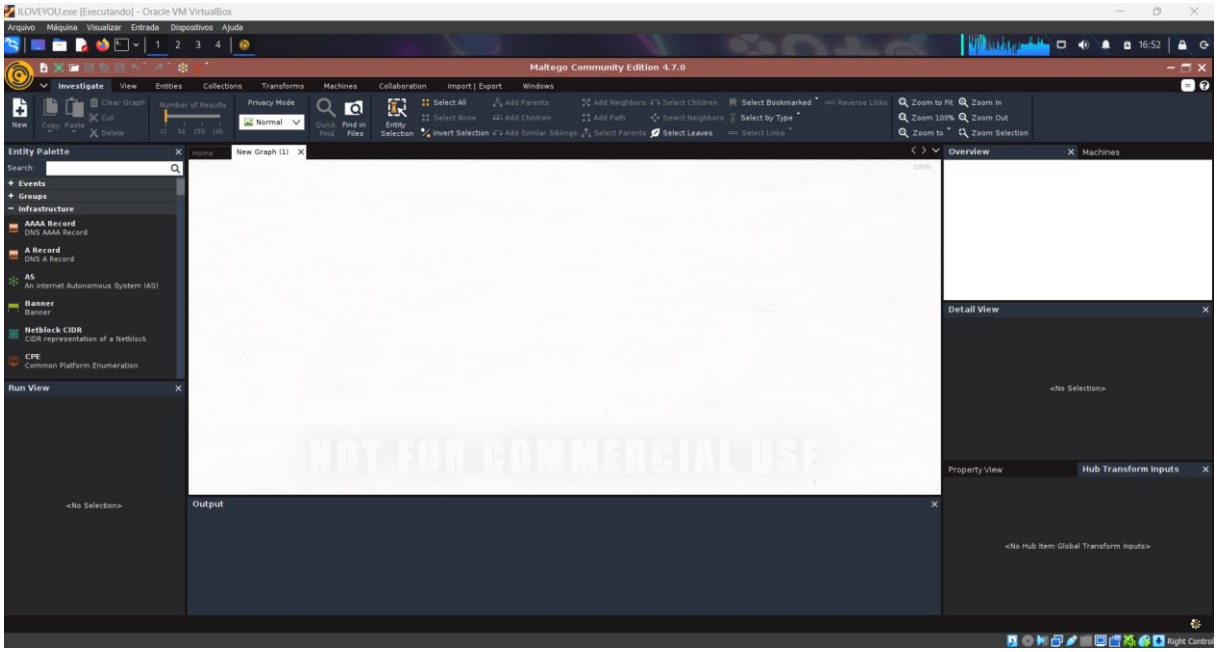
Quando abrir na página inicial, aparecerá essa tela:



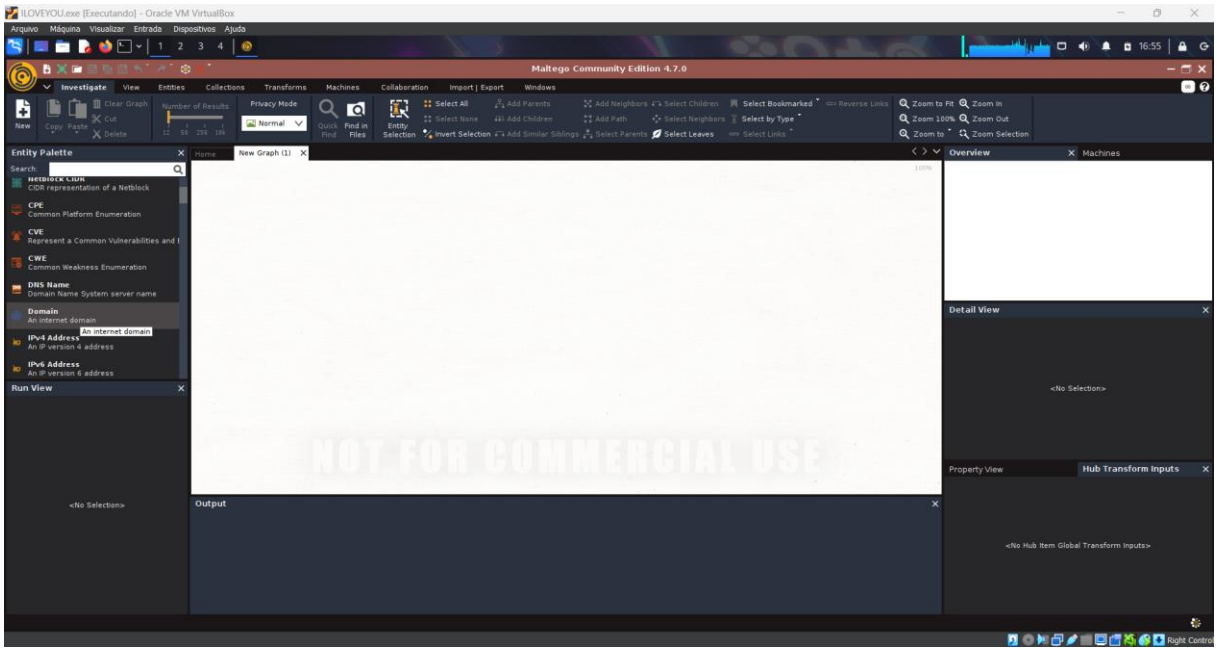

Vá em '*New*':



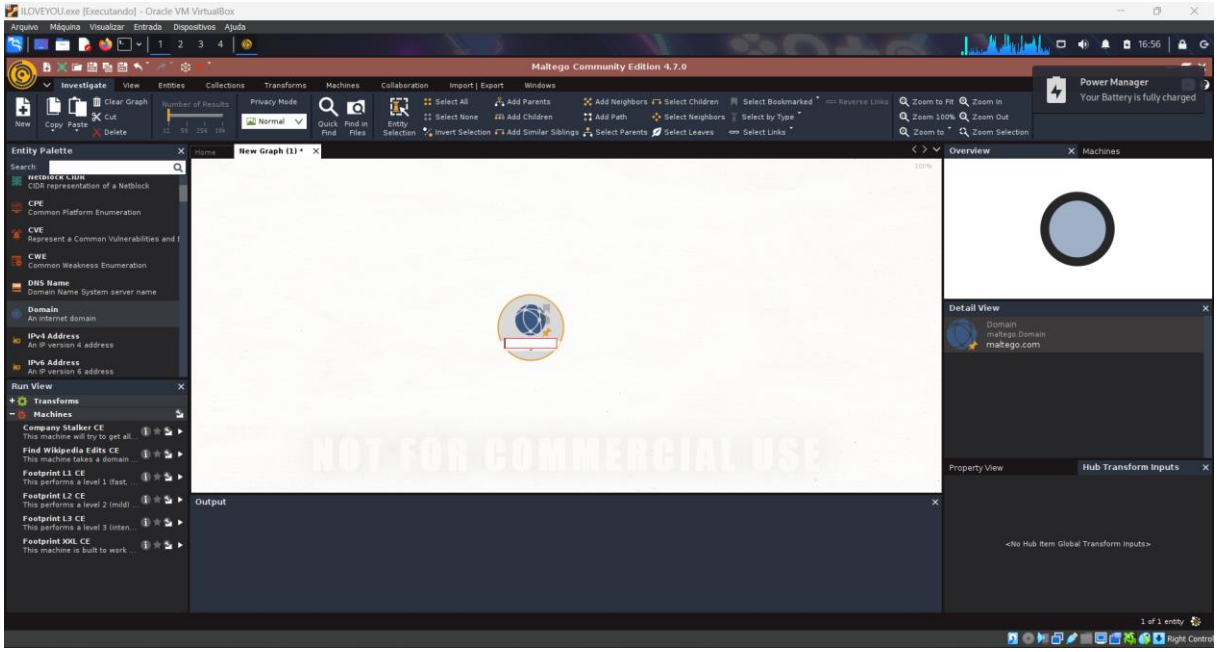

Abrirá um arquivo em branco. Vá na lista no canto lateral esquerdo da tela, chamado de *Entity Palette*, e procure *Infrastructure.*



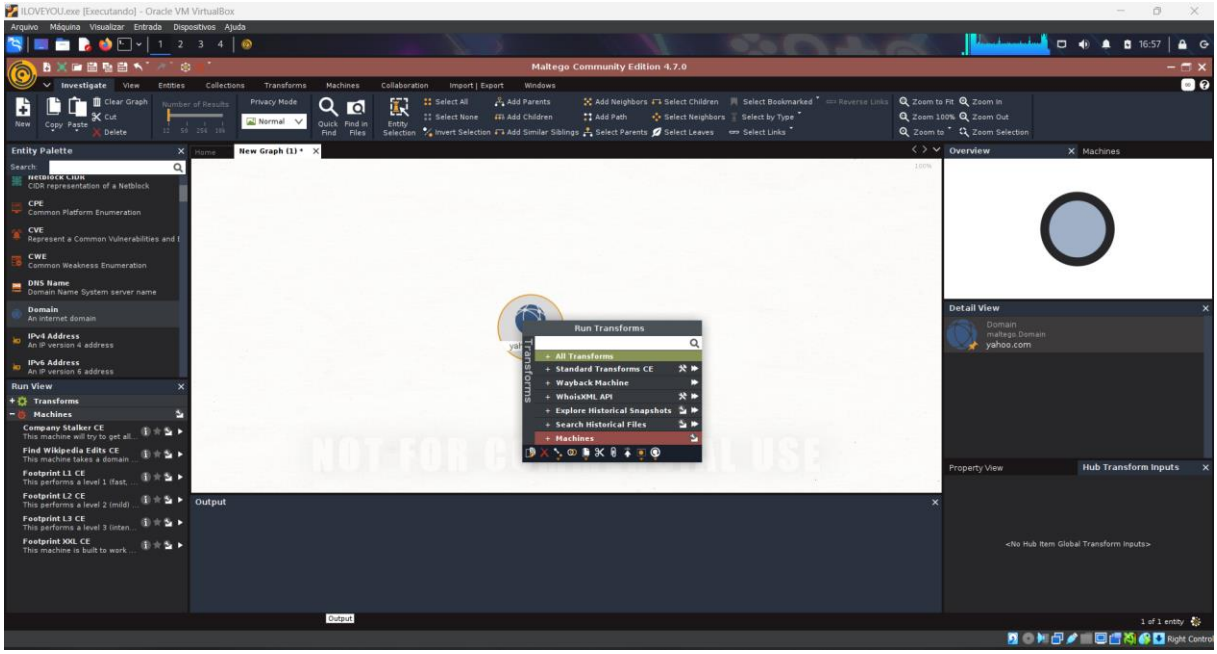

Agora procure uma figura de globo, com o nome *Domain*. Clique, segura e arraste.



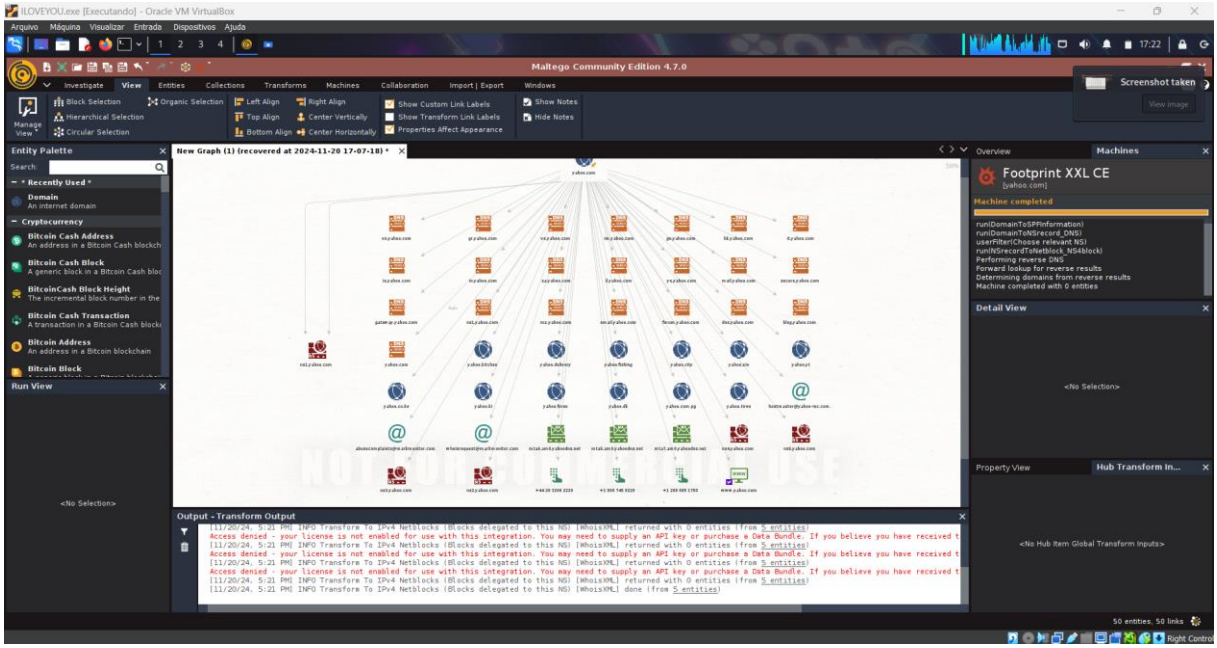

Clique e coloque o *link* de sua preferência.




No exemplo, foi utilizado *yahoo.com*. Depois, clique com o botão direito do *mouse*, e clique nessas setas, baseado no que você quer saber sobre o *site*.




No exemplo, executamos tudo. O que foi encontrado todos esses dados, indo de *DNS* e subdomínios, até *e-mails* etc.


ILOVEYOU.exe [Executando] - Oracle VM VirtualBox
Maltego Community Edition 4.7.0
Screenshot taken
Entity Palette
New Graph (1) (recovered at 2024-11-20 17-07-18) *
Overview
Machines
Footprint XXL CE
[yahoo.com]
Machine completed
Detail View
<No Selection>
Property View
Hub Transform In...
<No Hub Item Global Transform Inputs>
Run View
<No Selection>
Output - Transform Output
50 entities, 50 links

# CAPÍTULO 3. RESULTADOS E DISCUSSÃO

## 1. Resultado das ferramentas aplicadas

Na utilização prática, usamos ferramentas como o *Social Engineering Toolkit, GoPhish, BeEF, MalteGo e Recon-ng* para simular ataques de engenharia social. Os cenários usados foram: Simulação de *phishing* por e-mail e exploração de vulnerabilidades por links maliciosos. Verificamos que:

- Ao usar o BeEF, demonstrou-se que navegador desatualizado são um problema para ataques, reforçando a necessidade de políticas de atualização, além do problema humano de falta de conscientização, pois é preciso corrigir patches com frequência, o que são presentes nessas atualizações, para prevenir novas técnicas de ataques, tornando navegadores antigos mais vulneráveis.

As discussões que podem estar presentes nesse artigo são:

Foi verificado que o maior fator para o sucesso nos ataques são o desconhecimento dos usuários. Por isso, faz-se importante treinamentos, como no site *KnowBe4* ou na norma *NIST*. Além disso, é estritamente importante também a presença de um *MFA*, para impedir ataques de escalonamento de privilégios. Em quase todos os ataques comuns de engenharia social, a exploração de credenciais humanas normalmente é o ponto inicial.

Relacionado a reflexão da legislação brasileira, o *LGPD* e o Marco Civil da Internet tem bases sólidas para tratar essas violações, mas há um problema: na prática, ainda tem uma baixa fiscalização e falta de treinamento nas empresas. Integração entre treinamentos obrigatórios e auditorias externas regulares são recomendados, para aliviar esse problema.

# CONCLUSÃO

Ao ser usada a segurança da informação sobre a ótica da prevenção, mitigação e execução ética em relação do que tange a Engenharia Social, se demonstra continuamente um dos desafios latentes e existentes na contemporaneidade, especialmente se levarmos em consideração o avanço das novas tecnologias. Como visto nesse trabalho, demonstrou-se que o problema maior para o avanço da engenharia social de forma antiética não depende única e exclusivamente das vulnerabilidades dos sistemas e tecnologias, mas principalmente dos fatores humanos, utilizando técnicas de manipulação psicológica clássicas e funcionais para obter informações confidenciais e invadir sistemas não autorizados. Diante desse cenário, se faz importante as estratégias de prevenção e mitigação, como o uso das autenticações multifator, treinamento baseado na norma NIST, o cumprimento das leis brasileiras como a Lei Geral de Proteção de Dados (LGPD), Estratégia de Governança Digital (EGD), Decreto nº 9.637/2018 - Política Nacional de Segurança da Informação, Estratégia Nacional de Segurança Cibernética (E-Ciber) e a Instrução Normativa nº1/DSIC/GSIPR, o cumprimento das família das normas ISO 27000, servem perfeitamente para treinar os colaboradores para maior controle de segurança organizacional.

O uso das *Security Technical Implementation Guides (STIGs)* e das políticas de controle de acesso renomados, como William Stallings, David Ferraiolo, Ravi S. Sandhu, Karen Scarfone, Eugene Howard Spafford e outros. Além disso, testes periódicos com os funcionários avaliam sua capacidade de identificar e evitar tentativas de engenharia social dentro da empresa, reforçando sua resiliência sobre possíveis incidentes, seus aprendizados e que todos sejam informados sobre o papel dessas simulações, o que complementa fortemente a *NIST e a ISO* citados anteriormente. Quando acompanhado com treinamentos corretivos, influencia fortemente a cultura de segurança organizacional.

Em síntese, esses três fatores combinados, bem como a integração entre tecnologia, processos e edu básicos da segurança da informação, a confidencialidade, integridade e disponibilidade dos dados.

# REFERÊNCIAS

ABIN, Agência Brasileira de Inteligência. Engenharia social. Guia para Proteção de Conhecimentos Sensíveis. Disponível em: https://www.gov.br/abin/pt-br/acesso-a-informacao/acoes-e-programas/PNPC/boaspraticas/cartilha-engenharia-social-guia-para-protecao-de-conhecimentos-sensiveis. Acesso em: 12 set. 2024.

ALEXANDER, Jason. Phishing Attacks: How They Work and How to Stop Them. Journal of Cybersecurity, v. 5, n. 3, p. 89-103, 2020.

ANDERSON, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3. ed. New York: Wiley, 2020.

BISHOP, Matt. Introduction to Computer Security. Boston: Addison-Wesley, 2004.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 out. 2024.

CAMACHO, Diego; MORALES, Dario. SET (Social-Engineer Toolkit) em Kali Linux. Revista Nexos Científicos, v. 5, n. 1, p. 9-16, 2021. Disponível em: https://nexoscientificos.vidanueva.edu.ec/index.php/ojs/article/view/40/164. Acesso em: 12 set. 2024.

CIALDINI, Robert B. Influência: A Psicologia da Persuasão. Rio de Janeiro: Campus, 2001.

CLARK, Ben; DOWNER, Nick. RTFM: Red Team Field Manual. V.2. Editora Independente, 11 jul. 2022.

CLOUDFLARE. Princípio do Menor Privilégio. Disponível em: https://www.cloudflare.com/pt-br/learning/access-management/principle-of-least-privilege/. Acesso em: 25 out. 2024.

Cybersecurity & Infrastructure Security Agency (CISA). Understanding and Mitigating Insider Threats. Disponível em: https://old.unifiedcompliance.com/products/search-authority-documents/authority-document/0001131/. Acesso em: 23 out. 2024.

DEFENSE INFORMATION SYSTEMS AGENCY (DISA). Security Technical Implementation Guides (STIGs). 2021. Disponível em: https://public.cyber.mil/stigs/. Acesso em: 15 out. 2024.

ESTADOS UNIDOS. Defense Information Systems Agency (DISA). Access Control STIG, Version 2, Release 3. Disponível em: https://old.unifiedcompliance.com/products/search-authority-documents/authority-document/0001131/. Acesso em: 25 out. 2024.

ESTADOS UNIDOS. Defense Information Systems Agency (DISA). Control AU-2: Audit and Accountability. Disponível em: https://www.stigviewer.com/controls/800-53/AU-2. Acesso em: 25 out. 2024.

ESTADOS UNIDOS. Defense Information Systems Agency (DISA). Email Services Policy STIG. Disponível em: https://www.stigviewer.com/stig/email_services_policy/. Acesso em: 18 out. 2024.

ESTADOS UNIDOS. Defense Information Systems Agency (DISA). Microsoft Outlook 2016 Security Technical Implementation Guide. Disponível em: https://www.stigviewer.com/stig/microsoft_outlook_2016. Acesso em: 18 out. 2024.

ESTADOS UNIDOS. Defense Information Systems Agency. Unified Endpoint Management Server Security Requirements Guide. Disponível em: https://www.stigviewer.com/stig/unified_endpoint_management_server_security_requirements_guide/. Acesso em: 23 out. 2024.

ESTADOS UNIDOS. Defense Information Systems Agency. Windows Defender Antivirus Security Technical Implementation Guide. Disponível em: https://www.stigviewer.com/stig/windows_defender_antivirus/. Acesso em: 23 out. 2024.

EURICH, Peter; PABST, Kevin. The Financial and Legal Impact of Cyber Attacks. Cham: Springer, 2022.

GRASSI, Paul A. et al. NIST Special Publication 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management. National Institute of Standards and Technology, 2017. Disponível em: https://pages.nist.gov/800-63-3/sp800-63b.html. Acesso em: 23 set. 2024.

HADNAGY, Christopher. Social Engineering, The Science of Human Hacking. 2. ed. Hoboken: Wiley Editora, 2018.

HERLEY, Cormac. The Economics of Information Security: Human Vulnerabilities and Social Engineering. Computers & Security, v. 100, p. 102-113, 2021.

IBM. Cost of a Data Breach Report 2023. Disponível em: https://www.ibm.com/security/data-breach. Acesso em: 15 set. 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements. 2013. Disponível em: https://www.iso.org/standard/54534.html. Acesso em: 15 out. 2024.

ISO/IEC 27001:2013. Tecnologia da Informação — Técnicas de Segurança — Sistemas de gestão da segurança da informação — Requisitos. Brasília: Associação Brasileira de Normas Técnicas, 2013. Disponível em: https://manuais.satc.edu.br/lib/exe/fetch.php?media=iso:iso_iec_27001.pdf. Acesso em: 14 set 2024.

ISO/IEC 27002:2022. International Standard: Information security, cybersecurity and privacy protection — Information security controls. Suiça: International Organization for Standardization. Disponível em https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.itref.ir/uploads/editor/d3d149.pdf&ved=2ahUKEwjqg-fW2MiIAxVrlZUCHfE3OgsQFnoECAgQAQ&usg=AOvVaw27mhMdqeYXkye5zEGslDEa. Acesso em 15 set 2024.

JAKOBSSON, Markus; MYERS, Steven (Eds.). Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. New York: Wiley-Interscience, 2006

KAUFMAN, Charlie et al. Network Security: Private Communication in a Public World. 2. ed. Boston: Prentice Hall, 2022.

LONGTCHI, Theodore Tangie et al. Internet-Based Social Engineering Psychology, Attacks, and Defenses: A Survey. Proceedings of the IEEE, vol. 112, no. 3, pp. 210-246, março 2024. Disponível em https://ieeexplore.ieee.org/document/10493072. Acesso em 12 set. 2024.

MICROSOFT. Security Guidance and MFA Impact. Microsoft, 2019.

MILLER, David et al. Security Information and Event Management (SIEM) Implementation. 1. ed. Birmingham: Packt Publishing, 2010.

MITNICK, Kevin D.; SIMON, William L. A arte de enganar. 1. ed. São Paulo: Pearson, 2003.

MORENO, Daniel. Pentest em Aplicações Web. 1. ed. São Paulo: Novatec Editora, 2017.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Computer Security Incident Handling Guide. NIST Special Publication 800-61. 2018. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. Acesso em: 15 out. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. NIST Special Publication 800-161 Revision 1, 2022. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf. Acesso em: 15 out. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Guidelines for Media Sanitization. NIST Special Publication 800-88. 2014. Disponível em:

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf. Acesso em: 15 out. 2024.

NIST (National Institute of Standards and Technology). Building an Information Technology Security Awareness and Training Program. Gaithersburg: NIST, 2003. (NIST Special Publication 800-50). Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf. Acesso em: 08 out. 2024.

PELTIER, Thomas R. Information Security Fundamentals. 2. ed. Auerbach Publications, 2013.

SANS INSTITUTE. Social Engineering Attacks: Common Techniques & How to Prevent an Attack. SANS Whitepaper, 2019. Disponível em: https://www.sans.org.

SCARFONE, Karen; SOUPPAYA, Murugiah; Guide to Computer Security Log Management. NIST Special Publication 800-92, 2006. Disponível em https://www.nist.gov/publications/guide-computer-security-log-management. Acesso em: 15 out. 2024.

SCARFONE, Karen; SOUPPAYA, Murugiah; Guide to Enterprise Patch Management Technologies. NIST Special Publication 800-40 Revision 3, 2013. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf. Acesso em: 15 out. 2024.

SCHEIN, Edgar H; SCHEIN, Peter A. Organizational Culture and Leadership. 5. ed. San Francisco: Jossey-Bass, 2016.

SOUZA, Raul Carvalho de. Prevenção para ataques de engenharia social: um estudo sobre a confiança em segurança da informação em uma ótica objetiva, social, estrutural e interdisciplinar. 2015. [Tese (Doutorado em Engenharia de Sistemas e Computação)] – Universidade de Brasília, Brasília, 2015. Disponível em: http://www.realp.unb.br/jspui/bitstream/10482/18863/1/2015_RaulCarvalhodeSouza.pdf. Acesso em: 12 set. 2024.

STAJANO, Frank; WILSON, Paul. Understanding Scan Victims: Seven Principles for Systems Security. Communications of the ACM. v. 54, n. 3. Disponível em https://dl.acm.org/doi/pdf/10.1145/1897852.1897872. Acesso em 12 set. 2024.

STALLINGS, William; BROWN, Lawrie. Segurança de computadores: princípios e práticas. 2. ed. São Paulo: Pearson Prentice Hall, 2013.

STAMP, Mark. Information Security: Principles and Practice. 3. ed. New York: Wiley, 2021.

STEWART, J. Michael; KINSEY, Denise. Network Security, Firewalls, and VPNs. 3. ed. Burlington: Jones & Bartlett Learning, 2020.

SYMANTEC. Internet Security Threat Report. Symantec, 2021. Disponível em: https://www.symantec.com.

TIESO, Igor Henrique de Souza. Ataques de engenharia social. Revista Interface Tecnológica, v. 17, n. 2, p. 1-10, 2020. Disponível em: https://revista.fatectq.edu.br/index.php/interfacetecnologica/article/view/947. Acesso em: 12 set. 2024.

VERIZON. Data Breach Investigations Report 2023. Disponível em: https://www.verizon.com/business/resources/reports/dbir/. Acesso em: 15 set. 2024.

WRIGHT, Richard; WILLIAMS, Michael. Advances in Social Engineering and Cybersecurity. London: Routledge, 2023.

YAWOSKI, Peter. Real-World Bug Hunting: A Field Guide to Web Hacking. São Francisco: No Starch Press, 2020.